

A New Identity of Dickson Polynomials

Antonia W. Blüher

October 20, 2016

Abstract

We find a new polynomial identity in characteristic 2:

$$\prod_{w \in \mathbb{F}_q^\times} (D_{q+1}(wX) - Y) = X^{q^2-1} + \left(\sum_{i=1}^n Y^{2^n-2^i} \right) X^{q-1} + Y^{q-1},$$

where $q = 2^n$ and D_k is a Dickson polynomial, defined by $D_k(u+u^{-1}) = u^k + u^{-k}$. Using this identity, we prove that if F is a field of characteristic 2 and a is a nonzero element of F , then for $q = 2^n > 2$, the two polynomials $x^{q+1} + x + 1/a$ and $C(x) + a$ have the same splitting field over F , where $C(x) = x(\sum_{i=0}^{n-1} x^{2^i-1})^{q+1}$ is a Müller–Cohen–Matthews polynomial of degree $(q^2 - q)/2$. We find explicit formulas for how the roots of the two polynomials are related, and for the action of the Galois group. As a result, we can describe precisely how the factorizations of the two polynomials are related in the case where F is finite. In addition, we obtain a new proof of the known result that $C(x)$ induces a permutation on \mathbb{F}_{2^m} if $2m$ and n are relatively prime.

1. Introduction

We find a new polynomial identity in characteristic 2:

$$\prod_{w \in \mathbb{F}_q^\times} (D_{q+1}(wX) - Y) = X^{q^2-1} + \left(\sum_{i=1}^n Y^{2^n-2^i} \right) X^{q-1} + Y^{q-1}, \quad (1)$$

where $q = 2^n$ and D_k is a Dickson polynomial, defined by $D_k(u+u^{-1}) = u^k + u^{-k}$. Using this identity, we prove that if F is a field of characteristic 2 and a is a nonzero element of F , then for $q = 2^n > 2$, the two polynomials $x^{q+1} + x + 1/a$ and $C(x) + a$ have the same splitting field over F , where $C(x) = x(\sum_{i=0}^{n-1} x^{2^i-1})^{q+1}$ is a Müller–Cohen–Matthews polynomial of degree $(q^2 - q)/2$. We find explicit formulas relating the roots of the two polynomials, and we describe the Galois action. As a result, when F is finite, related factorizations of the two polynomials can be explained. We also found a new proof that $C(x)$ induces a permutation on \mathbb{F}_{2^m} if $(2m, n) = 1$. (See [2] for the original proof. A polynomial that induces a permutation on infinitely many finite fields is said to be *exceptional*.)

A first draft of this article was written in the 2001–2004 timeframe, but was left and forgotten for over a decade. The project was resumed and completed in 2016,

with the following improvements. A hypothesis that the field F must be perfect was removed, the new proof of exceptionality of $C(x)$ was added, a simpler formula was found for the roots of $C(x)$, and a simpler description of dihedral subgroups of $\mathrm{PGL}_2(q)$ was obtained (see Proposition 6.1; an analogous proposition holds for q odd as well.) Finally, references were updated to reflect advances in the understanding of exceptional polynomials that occurred in the intervening decade.

A few remarks are in order. First, the equality of the splitting fields of the two polynomials $x^{q+1} + x + 1/a$ and $C(x) + a$ can be derived from work of Zieve [9] and Lenstra and Zieve [8], at least in the case where a is transcendental. Many calculations in this paper could perhaps be done more expediently with their methods, which utilize group theory. However, the author was unaware of these methods at the time that she carried out her work, and as a result she used different techniques and was motivated by a different set of questions. We hope that this new perspective will complement the existing literature.

The polynomial identity involving Dickson polynomials in characteristic 2 is new. It seems to apply only to characteristic 2. Bob Guralnick points out that the Dickson polynomials are ramified at the prime 2, thus it is not surprising to find formulas that are special to characteristic 2.

The results in our paper seem related to but different from results in Abhyankar, Cohen, and Zieve [1]. Both our paper and theirs give a factorization of $x^{q^2-1} - a(y)x^{q-1} - b(y)$ in terms of Dickson polynomials and use it to deduce information about the Galois groups of certain polynomials. However, the functions $a(y)$ and $b(y)$ differ, and so do the Galois groups that are involved. Their identity generalizes to all characteristics, whereas ours applies only to characteristic 2. A precise statement of the identity in [1] is given in the remark preceding Lemma 2.3. It would be interesting to understand more fully how the two polynomial identities are related.

Finally, we mention that in one case, our work fits nicely with results of Dummit [4] on solvable quintics. Namely, $x^{q+1} + x + 1/a$ is a quintic when $q = 4$. Dummit notes that a quintic (over any field) is solvable if and only if its Galois group is contained in a group that is conjugate to F_{20} , where $F_{20} \subset S_5$ is generated by the permutations (12345) and (2354). It turns out that an invariant θ for F_{20} is given by:

$$\begin{aligned} \theta = & x_1^2 x_2 x_5 + x_1^2 x_3 x_4 + x_2^2 x_1 x_3 + x_2^2 x_4 x_5 + x_3^2 x_1 x_5 \\ & + x_3^2 x_2 x_4 + x_4^2 x_1 x_2 + x_4^2 x_3 x_5 + x_5^2 x_1 x_4 + x_5^2 x_2 x_3, \end{aligned}$$

where x_i are the roots of the quintic. Let $\gamma_1, \dots, \gamma_6$ be coset representatives for S_5/F_{20} . Then $\prod_{i=1}^6 (x - \gamma_i(\theta))$ is a sextic. In the case of the polynomial $x^5 + x + 1/a$ in characteristic 2, the sextic is equal to $x^6 + a^{-4}x + a^{-4}$. Setting $y = 1/x$, we see that this is equivalent (has the same splitting field) to $y^6 + y^5 + a^4$. If we set $y = z^4$ and then take a fourth root, this reduces to our function $z^5(z + 1) + a$. The substitution $z \mapsto z + 1$ brings it to the form $C(z) + a$. The above expression for θ shows explicitly in this case how the roots of $C(x) + a$ are related to the roots of the quintic.

The relation between the roots causes a relation between the factorizations of the two polynomials. Write $f \sim [n_1, n_2, \dots, n_t]$ if f factors into irreducibles of degrees n_1, n_2, \dots, n_t . When $q = 4$ and $F = \mathbb{F}_{2^k}$, we will prove the following in Section 6.

Proposition 1.1 *For k even, x^5+x+1/a has one of these factorization types: $[1, 1, 1, 1, 1]$, $[1, 1, 3]$, $[1, 2, 2]$, or $[5]$. We have*

$$\begin{aligned} x^5 + x + 1/a \sim [1, 1, 1, 1, 1] &\iff x(1+x)^5 + a \sim [1, 1, 1, 1, 1, 1] \\ x^5 + x + 1/a \sim [1, 1, 3] &\iff x(1+x)^5 + a \sim [3, 3] \\ x^5 + x + 1/a \sim [1, 2, 2] &\iff x(1+x)^5 + a \sim [1, 1, 2, 2] \\ x^5 + x + 1/a \sim [5] &\iff x(1+x)^5 + a \sim [1, 5]. \end{aligned}$$

For k odd, $x^5 + x + 1/a$ has factorization type $[1, 1, 1, 2]$, $[1, 4]$, or $[2, 3]$, and we have

$$\begin{aligned} x^5 + x + 1/a \sim [1, 1, 1, 2] &\iff x(1+x)^5 + a \sim [2, 2, 2] \\ x^5 + x + 1/a \sim [1, 4] &\iff x(1+x)^5 + a \sim [1, 1, 4] \\ x^5 + x + 1/a \sim [2, 3] &\iff x(1+x)^5 + a \sim [6]. \end{aligned}$$

The author wishes to thank John Dillon and Mike Zieve for their encouragement and for stimulating discussions. As a newcomer to the study of Galois groups and exceptional polynomials, the author found their expertise to be invaluable.

Notation. If R is a ring then R^\times denotes the group of units in R , and $R[x]$ denotes the ring of polynomials in the indeterminate x with coefficients in R . The separable algebraic closure of a field F is denoted \overline{F} . For a nonzero polynomial $f \in F[x]$, $\deg(f)$ is its degree, and $f_{rev}(x) = x^{\deg(f)} f(1/x)$ is the reverse of f . The splitting field of f over F is written $\text{SF}(f; F)$; this is the subfield of \overline{F} that is generated by F and by all the roots of f . The Galois group of $\text{SF}(f; F)$ over F is denoted by $\text{Gal}(f; F)$; it is the group of automorphisms of the field $\text{SF}(f; F)$ that fix the subfield F . If ℓ is a prime power, then \mathbb{F}_ℓ denotes the (unique) field with ℓ elements. For $k \geq 1$, $D_k(x)$ denotes the k -th Dickson polynomial, which is the unique monic polynomial of degree k such that $D_k(x + 1/x) = x^k + 1/x^k$.

Because the expression $x + 1/x$ arises so frequently in this article, we introduce the special notation:

$$\langle x \rangle = x + 1/x.$$

Then the defining property of the Dickson polynomial may be written as

$$D_k(\langle x \rangle) = \langle x^k \rangle.$$

Note that

$$\langle 1/x \rangle = \langle x \rangle \tag{2}$$

$$\langle x \rangle \langle y \rangle = \langle xy \rangle + \langle x/y \rangle$$

$$\langle x \rangle \langle y/z \rangle = \langle xy \rangle \langle z \rangle + \langle xz \rangle \langle y \rangle \quad \text{in char. } 2 \tag{3}$$

$$\langle x^{p^i} \rangle = \langle x \rangle^{p^i} \quad \text{in char. } p. \tag{4}$$

We use the following notation that is specific to this article:

$$q = 2^n, \quad \text{where } n > 1.$$

$$T(x) = \sum_{i=0}^{n-1} x^{2^i-1}, \quad T_{rev}(x) = \sum_{i=0}^{n-1} x^{(q/2)-2^i}$$

$$C(x) = x \cdot T(x)^{q+1} \quad (\text{a Müller–Cohen–Matthews polynomial})$$

F is a field of char. 2 and a is a fixed nonzero element of F

$$\mu_k = \{\zeta \in \overline{\mathbb{F}}_2^\times : \zeta^k = 1\}$$

$$K = \text{SF}(C(x) + a; F)$$

$$L = \text{SF}(x^{q+1} + x + 1/a; F).$$

$$\mathbb{F}_{q,1} = \{d \in \mathbb{F}_q : \text{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(d) = 1\}, \quad \mathbb{F}_{q,0} = \{d \in \mathbb{F}_q : \text{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(d) = 0\}.$$

If $f(x)$ is a polynomial and its irreducible factors have degrees d_1, d_2, \dots, d_k then we write $f \sim [d_1, d_2, \dots, d_k]$.

In Section 3 only we allow $q = p^n$ and F has char. p , where p is any prime. We make frequent use of elements $\zeta \in \mu_{q+1}$. Since $q+1$ divides q^2-1 , we know $\zeta \in \mathbb{F}_{q^2}$. Note that $N_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\zeta) = \zeta\zeta^q = 1$, and $\text{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\zeta) = \zeta + \zeta^q = \zeta + \zeta^{-1} = \langle \zeta \rangle$.

Remark. If one assumes that F is perfect, then replacing all the coefficients of f by their 2^i -th powers does not affect the splitting field or Galois group. For example, the substitution $x \mapsto x/a$ transforms the polynomial $x^{q+1} + x + 1/a$ into $x^{q+1} + a^q x + a^q$, and this has the same automorphism group as the polynomial $x^{q+1} + ax + a$. In this article, we do not assume that F is perfect, but we are still able to show in Proposition 3.3 that the polynomials $x^{q+1} + x + 1/a$ and $x^{q+1} + ax + a$ have the same splitting field. The latter polynomial turns out to be the most convenient for the purpose of proving that these polynomials have the same splitting field as $C(x) + a$.

The article is organized as follows. Section 2 proves the Dickson polynomial identity. Section 3 concerns $x^{q+1} + ax + a$. It reviews results from [5] and proves a few additional results. For example, we show that $x^{q+1} + x + 1/a$ has the same splitting field as $x^{q+1} + ax + a$, without having to assume that F is perfect. Sections 4 and 5 prove that $K = L$ by explicitly writing the roots of $C(x) + a$ as a rational function of the roots of $x^{q+1} + ax + a$, and explicitly writing the roots of $x^{q+1} + ax + a$ in terms of the roots of $C(x) + a$. Also the following polynomial identity is derived:

$$\prod_{c \in \mathbb{F}_q^\times, j \in \mathbb{F}_{q,1}} (cy^2 + y + j/c) = 1 + (y^q + y)^{q-1}.$$

Section 6 considers the Galois group and shows how the factorizations of $x^{q+1} + x + 1/a$ and $C(x) + a$ are related. For example, we prove the related factorizations between $x^5 + x + 1/a$ and $x(x+1)^5 + a$ that were asserted in Proposition 1.1. Section 7 investigates dihedral groups of order $2(q+1)$ and shows that such groups fix a root of $C(x) + a$ in the geometric case. This is used in Section 8 to give a new proof that $C(x)$ is exceptional over \mathbb{F}_2 when n is odd.

2. An identity of Dickson polynomials

The k th Dickson polynomial is the monic polynomial with integer coefficients such that the formal identity holds, $D_k(u + 1/u) = u^k + 1/u^k$. To see that such a polynomial exists, note that $u^k + v^k$ is a polynomial in $u + v$ and uv by the Theorem of Symmetric Functions, say $u^k + v^k = F_k(u + v, uv)$. By setting $v = 1/u$, we find that $D_k(x) = F_k(x, 1)$. It is easy to see that $D_k(x)$ has degree k , and $D_k(-x) = (-1)^k D_k(x)$. Thus, if k is even then $D_k(x) = E_k(x^2)$, and if k is odd then $D_k(x) = xE_k(x^2)$, where E_k has degree $\lfloor k/2 \rfloor$. A useful relation is

$$D_k(x)D_\ell(x) = D_{k+\ell}(x) + D_{k-\ell}(x), \quad (5)$$

as can be seen from the identity $\langle u^k \rangle \langle u^\ell \rangle = \langle u^{k+\ell} \rangle + \langle u^{k-\ell} \rangle$.

Since D_k has integral coefficients, it can be considered over any field F , in any characteristic. If the characteristic is p , then

$$D_{kp^r}(x) = D_k(x)^{p^r}. \quad (6)$$

The complete set of roots of $D_k(x) - c$ is easy to construct. Namely, we find u so that $c = \langle u^k \rangle$; then $\langle u \rangle$ will be a root, and the other roots will be $\langle \zeta u \rangle$ for $\zeta \in \mu_k$. To find u , first solve the quadratic $v + 1/v = c$, then solve $v = u^k$.

We will need some well-known formulas for D_{q-1} and D_{q+1} in characteristic 2, where $q = 2^n$. For the reader's convenience, we include their proof below.

Lemma 2.1 *If $q = p^n$, then in characteristic p ,*

$$D_{q+1}(Y) = Y^{q+1} - D_{q-1}(Y).$$

If $q = 2^n$, then in characteristic 2,

$$D_{q-1}(Y) = \sum_{i=1}^n Y^{q-2^i+1}.$$

Proof. By (5), $D_q(Y)D_1(Y) = D_{q+1}(Y) + D_{q-1}(Y)$. By (6), $D_q(Y)D_1(Y) = Y^{q+1}$. Thus $D_{q+1}(Y) = Y^{q+1} - D_{q-1}(Y)$.

Now apply (5) with $k = 1$ and $\ell = q - 1$. We find that $YD_{q-1}(Y) = Y^q + D_{q-2}(Y)$. If $p = 2$, then this becomes

$$Y^q = YD_{q-1}(Y) + D_{(q/2)-1}(Y)^2.$$

Let $f_m = D_{2^m-1}(Y)$ and $g_m = \sum_{i=1}^m Y^{2^m-2^i+1}$. Then $f_1 = g_1 = Y$, $Yf_m = Y^{2^m} + f_{m-1}^2$ for $m \geq 2$, and $Yg_m = Y^{2^m} + g_{m-1}^2$ for $m \geq 2$. Thus $f_m = g_m$. ■

Theorem 2.2 *Let $q = 2^n$. In the polynomial ring $\mathbb{F}_q[X, Y]$ we have the identity:*

$$\prod_{w \in \mathbb{F}_q^\times} (D_{q+1}(wX) - Y) = X^{q^2-1} + \left(\sum_{i=1}^n Y^{2^n-2^i} \right) X^{q-1} + Y^{q-1}. \quad (7)$$

Proof. Let U be transcendental over \mathbb{F}_2 and

$$Y = \langle U^{q+1} \rangle$$

(where we recall $\langle u \rangle$ is shorthand for $u + 1/u$). Then Y is also transcendental, and $\mathbb{F}_2(Y) \subset \mathbb{F}_2(U)$. Let $L(X)$ and $R(X)$ denote the left-hand and right-hand sides of (7) respectively, considered as elements of $\overline{\mathbb{F}_2}(U)[X]$. Note that L and R are both monic polynomials in X of degree $q^2 - 1$, and so $\deg_X(L - R) < q^2 - 1$. Thus, to prove $L - R$ is identically zero it suffices to find $q^2 - 1$ distinct roots in $\overline{\mathbb{F}_2}(U)$. We claim that these roots are

$$\{ \langle \zeta U \rangle / w : \zeta \in \mu_{q+1} \text{ and } w \in \mathbb{F}_q^\times \}. \quad (8)$$

(The proof that these are distinct will be shown in Lemma 2.3 below.) In fact we will show that L and R each vanish at these values. Let x denote one of these values:

$$x = \langle \zeta U \rangle / w.$$

First, $L(x) = 0$ because

$$D_{q+1}(wx) - Y = D_{q+1}(\langle \zeta U \rangle) - Y = \langle (\zeta U)^{q+1} \rangle - \langle U^{q+1} \rangle = 0.$$

Next we show $R(x) = 0$. Set $V = \zeta U$; then

$$x = \langle V \rangle / w \quad \text{and} \quad Y = \langle V^{q+1} \rangle. \quad (9)$$

Note that $\langle V \rangle Y = \langle V \rangle \langle V^{q+1} \rangle$ is nonzero, since V is transcendental. Thus, it will suffice to show that $\langle V \rangle Y R(x) = 0$. Noting that $w^{q-1} = 1$ and invoking Lemma 2.1, we have

$$\begin{aligned} \langle V \rangle Y R(x) &= Y \langle V \rangle^{q^2} + \left(\sum_{i=1}^n Y^{2^n - 2^i + 1} \right) \langle V \rangle^q + \langle V \rangle Y^q \\ &= \langle V^{q+1} \rangle \langle V^{q^2} \rangle + D_{q-1}(Y) \langle V^q \rangle + \langle V \rangle \langle V^{q(q+1)} \rangle. \end{aligned}$$

Now $D_{q-1}(Y) = D_{q-1}(\langle V^{q+1} \rangle) = \langle (V^{q+1})^{q-1} \rangle = \langle V^{q^2-1} \rangle$. Using this observation and (5), we obtain

$$\begin{aligned} \langle V \rangle Y R(x) &= \langle V^{q+1} \rangle \langle V^{q^2} \rangle + \langle V^{q^2-1} \rangle \langle V^q \rangle + \langle V \rangle \langle V^{q(q+1)} \rangle \\ &= \langle V^{q^2+q+1} \rangle + \langle V^{q^2-q-1} \rangle + \langle V^{q^2+q-1} \rangle + \langle V^{q^2-q-1} \rangle + \langle V^{q^2+q+1} \rangle + \langle V^{q^2+q-1} \rangle \\ &= 0. \end{aligned}$$

Thus $R(x) = 0$, as claimed. \blacksquare

Remark. Our identity (7) is tantalizingly similar to an identity in Theorem (1.1) from the article by Abhyankar, Cohen, and Zieve [1]. Their identity is

$$X^{q^2-1} - E_q(Y, 1)X^{q-1} + E_{q-1}(Y, 1) = (X^{2q-2} - YX^{q-1} + 1) \left(\prod_{w \in \mathbb{F}_q^\times} (D_{q-1}(X, w) - Y) \right),$$

where $q = p^n$, $D_n(X, a)$ is defined by $D_n(U_1 + U_2, U_1 U_2) = U_1^n + U_2^n$, and $E_i(Y, a)$ is defined by $E_i(U_1 + U_2, U_1 U_2) = (U_1^{n+1} - U_2^{n+1})/(U_1 - U_2)$. Using the relations (2.20) and (2.9) of [1], this identity can be rewritten when $p = 2$ as:

$$X^{q^2-1} + (D_{q+1}(Y)/Y)X^{q-1} + Y^{q-1} = (X^{2q-2} - YX^{q-1} + 1) \left(\prod_{w \in \mathbb{F}_q^\times} (D_{q-1}(wX) - Y) \right),$$

and using Lemma 2.1, our identity can be rewritten as

$$X^{q^2-1} + (D_{q+1}(Y)/Y)X^{q-1} + Y^{q-1} = \prod_{w \in \mathbb{F}_q^\times} (D_{q+1}(wX) - Y).$$

In both this article and [1], the identity is used to compute a certain Galois group, which in this article turns out to be $\text{PSL}_2(q)$ and in [1] turns out to be an orthogonal group. Bob Guralnick points out that the Dickson polynomials are ramified at the prime 2, thus it is not surprising to find formulas that are special to characteristic 2.

The following result was needed in the proof of Theorem 2.2.

Lemma 2.3 *Let M be a field of characteristic 2 that strictly contains \mathbb{F}_{q^2} , and let $u \in M \setminus \mathbb{F}_{q^2}$. Then the values*

$$\{ \langle \zeta u \rangle / w : \zeta \in \mu_{q+1} \text{ and } w \in \mathbb{F}_q^\times \}$$

are distinct.

Proof. Let $\zeta, \lambda \in \mu_{q+1}$ and $w, w' \in \mathbb{F}_q$, and suppose that $\langle \zeta u \rangle / w = \langle \lambda u \rangle / w'$. Then $w/w' = \langle \zeta u \rangle / \langle \lambda u \rangle$, and so

$$\frac{\zeta w}{\lambda w'} = \frac{\zeta \langle \zeta u \rangle}{\lambda \langle \lambda u \rangle} = \frac{\zeta^2 u^2 + 1}{\lambda^2 u^2 + 1}.$$

If $\zeta \neq \lambda$, then we can solve for u^2 in terms of ζ, λ, w, w' , but this contradicts the hypothesis that $u \notin \mathbb{F}_{q^2}$. Thus, $\zeta = \lambda$, and consequently $w = w'$ also. We have shown that $\langle \zeta u \rangle / w = \langle \lambda u \rangle / w'$ implies $\zeta = \zeta'$ and $w = w'$, so the roots are distinct, as claimed.

■

For future use, we record the following lemma.

Lemma 2.4 *Let y be a nonzero element of a field M of characteristic 2, and let*

$$f(x) = \prod_{w \in \mathbb{F}_q^\times} (D_{q+1}(wx) - y).$$

Let $u \in \overline{M}$ satisfy $u^{q+1} + 1/u^{q+1} = y$. The complete set of roots of f is

$$\{ w \langle \zeta u \rangle : w \in \mathbb{F}_q^\times, \zeta \in \mu_{q+1} \}$$

and these roots are distinct.

Proof. By (7), $f = x^{q^2-1} + T_{rev}(y^2)x^{q-1} + y^{q-1}$. The roots of f are distinct, because $f - xf' = y^{q-1} \neq 0$ shows that $\text{GCD}(f, f') = 1$. Also the roots are nonzero, since the constant term of f is y^{q-1} . Now $D_{q+1}(wx) - y$ vanishes at $w^{-1}\langle \zeta u \rangle$, for all $\zeta \in \mu_{q+1}$. We claim the values $\langle \zeta u \rangle$ are distinct. If not, then $\langle \zeta u \rangle = \langle \zeta' u \rangle$ for distinct $\zeta, \zeta' \in \mu_{q+1}$. One finds that $u^2 = (1/\zeta' + 1/\zeta)/(\zeta + \zeta') = 1/(\zeta\zeta')$. Then $y^2 = \langle u^{2(q+1)} \rangle = \langle 1 \rangle = 0$, contrary to the hypothesis that y is nonzero. This establishes that the $q+1$ roots of $D_{q+1}(wx) - y$ given by $\{\langle \zeta u \rangle/w : \zeta \in \mu_{q+1}\}$ are distinct. Now the roots of $D_{q+1}(wx) - y$ must be disjoint from the roots of $D_{q+1}(w'x) - y$ when $w \neq w'$, since we already observed that f has no repeated roots. Thus, the $q^2 - 1$ roots given in the statement of the lemma are distinct, and since $\deg(f) = q^2 - 1$, we have found all the roots. ■

Now we show how the Dickson polynomial leads to a relation between the polynomials $C(x) + a$ and $x^{q+1} + ax + a$, where we recall that C is defined by

$$C(x) = x \cdot T(x)^{q+1}, \quad T(x) = \sum_{i=0}^{n-1} x^{2^i-1}.$$

Lemma 2.5 $C(x) + a$ has distinct roots over \overline{F} , all nonzero.

Proof. A polynomial has distinct roots over the algebraic closure if and only if it is relatively prime to its derivative. Since $C = xT^{q+1}$ and $xC' = T^{q+1} + (q+1)xT^qT' = T^{q+1} + T^{q+1} = 2T^{q+1}$, we see that $C' = T^q(xT' + T) = T^q$, which divides C . Setting $G(x) = C(x) + a$, we have $G' = C' = C/(xT)$, and so $G - xTG' = (C + a) - C = a$. This proves that $\text{GCD}(G, G') = 1$, and so $C(x) + a$ has no repeated roots. Since $C(0) + a = a \neq 0$, the roots are nonzero. ■

For the remainder of this section, let e be an arbitrary root of $C(x) + a$:

$$C(e) = a.$$

Proposition 2.6 Let $u \in \overline{F}$ satisfy

$$u^{q+1} + 1/u^{q+1} = 1/e.$$

Then the complete set of roots of $x^{q+1} + a^2x + a^2$ is

$$\{ eT(e)^2 \langle \zeta u \rangle^{q-1} : \zeta \in \mu_{q+1} \}.$$

Proof. Substitute $Y = 1/e$ into the identity (7) and leave X as an indeterminate. We find:

$$\prod_{w \in \mathbb{F}_q^\times} (D_{q+1}(wX) - 1/e) = X^{q^2-1} + \alpha X^{q-1} + \beta,$$

where

$$\alpha = \sum_{i=1}^n e^{2^i-q} = (eT(e))^2/e^q = e^{2-q}T(e)^2, \quad \beta = e^{1-q}.$$

Let

$$R = (\alpha/\beta)X^{q-1} = eT(e)^2X^{q-1}.$$

Then, the right side of the identity can be written as $(\beta/\alpha)^{q+1}(R^{q+1} + \alpha^{q+1}/\beta^q R + \alpha^{q+1}/\beta^q)$. Now $\alpha^{q+1}/\beta^q = e^2 T(e)^{2(q+1)} = C(e)^2 = a^2$, and so we have the identity:

$$\prod_{w \in \mathbb{F}_q^\times} (D_{q+1}(wX) - 1/e) = (\beta/\alpha)^{q+1}(R^{q+1} + a^2 R + a^2).$$

By Lemma 2.4, the roots of the left side are $w\langle\zeta u\rangle$ for $\zeta \in \mu_{q+1}$ and $w \in \mathbb{F}_q^\times$, and these are distinct. Denote the set of these roots by S ; we have $|S| = q^2 - 1$, and also $s \in S$ implies $ws \in S$ for all $w \in \mathbb{F}_q^\times$. If $s_1, s_2 \in S$ then $s_1^{q-1} = s_2^{q-1}$ if and only if $s_1/s_2 \in \mathbb{F}_q^\times$. Thus, each power s^{q-1} has exactly $q - 1$ preimages in S , namely $\{ws : w \in \mathbb{F}_q^\times\}$. It follows that there are exactly $q+1$ distinct values $\{s^{q-1} : s \in S\} = \{\langle\zeta u\rangle^{q-1} : \zeta \in \mu_{q+1}\}$. This shows that the values $\langle\zeta u\rangle^{q-1}$ are distinct. Since $R = eT(e)^2 X^{q-1}$, it follows that $eT(e)^2 \langle\zeta u\rangle^{q-1}$ are roots of $R^{q+1} + a^2 R + a^2$, and since they are distinct, all $q+1$ roots are accounted for. ■

3. Splitting field of $x^{q+1} - bx + b$.

For this section only, we will consider both even and odd characteristic. Let p be a prime and $q = p^n$. The polynomial $f(x) = x^{q+1} - bx + b$ in characteristic p (where $b \neq 0$) was studied in [5]. More generally, one could begin with $x^{q+1} + Ax^q + Bx + C$ (where $(AB - C)(B - A^q) \neq 0$), and the substitution $x = (AB - C)(B - A^q)^{-1}x_1 - A$ brings us to the “standard” form $x_1^{q+1} - bx_1 + b$, where $b \neq 0$. The polynomial $x^{q+1} + a^2x + a^2$ that arises in Proposition 2.6 is just the special case $p = 2$, $b = a^2$. The article [5] gives explicit formulas for the splitting field and for the Galois action, which we recall in Theorems 3.1 and 3.2 below. Theorem 3.1 is illustrated in Figure 3.

Theorem 3.1 ([5]) *Let $q = p^n$ and let b be a nonzero of a field F in char. p . Let r, r_0, r_1 be distinct roots of $x^{q+1} - bx + b$, and define*

$$z = r_0/r, \quad y = (r_1 - r)/(r_1 - r_0), \quad \xi = y^q - y. \quad (10)$$

Then

$$y^{q-1} = z, \quad \xi = y(z - 1), \quad \text{and} \quad z(z - 1)^{q-1} = 1/(r - 1) = \xi^{q-1}.$$

We have $y^{q^2} - y = \xi^q + \xi \neq 0$.

Proof. Although the proof can be found in [5], we include it here because it is so short. First, $rr_0(r - r_0)^q = r_0r^{q+1} - rr_0^{q+1} = r_0b(r - 1) - rb(r_0 - 1) = b(r - r_0)$, so

$$b = rr_0(r - r_0)^{q-1}.$$

Dividing through by r^{q+1} and using $r^{q+1} = b(r - 1)$, we find $1/(r - 1) = z(z - 1)^{q-1}$. Next, from $b = r_1r_0(r_1 - r_0)^{q-1} = r_1r(r_1 - r)^{q-1}$ we find $1 = (r_1r_0/r_1r)((r_1 - r_0)/(r_1 - r))^{q-1} = zy^{1-q}$, so $z = y^{q-1}$. We have $\xi = y^q - y = y(z - 1)$, and so $\xi^{q-1} = y^{q-1}(z - 1)^{q-1} = z(z - 1)^{q-1} = 1/(r - 1)$. Note that $\xi \neq 0$ and $\xi^{q-1} \neq -1$, since $\xi^{q-1} = 1/(r - 1)$. Thus $\xi^q + \xi \neq 0$. ■

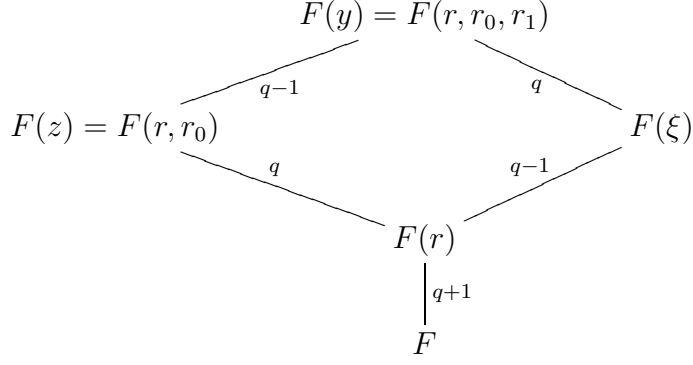


Figure 1: Splitting field of $x^{q+1} - bx + b$ when $F = \mathbb{F}_q(b)$ and b is transcendental. Here r, r_0, r_1 are roots of f , $y = (r_1 - r)/(r_1 - r_0)$, $z = y^{q-1}$, $\xi = y^q - y$, $\xi^{q-1} = z(z-1)^{q-1} = 1/(r-1)$, $r_0 = rz$, $r_1 = r(y-1)^{q-1}$. The degree of each extension field is indicated. The minimal polynomial for y over $F(z)$ is $y^{q-1} - z$. The minimal polynomial for y over $F(\xi)$ is $y^q - y - \xi$. The minimal polynomial for z over $F(r)$ is $z(z-1)^{q-1} - 1/(r-1)$. The minimal polynomial for ξ over $F(r)$ is $\xi^{q-1} - 1/(r-1)$. The minimal polynomial for r over F is $r^{q+1} - br + b$.

Theorem 3.2 *Let $f(x) = x^{q+1} - bx + b$. The complete set of roots of f is $\{r_w : w \in \mathbb{P}^1(q)\}$, where $r_\infty = r$ and $r_w = r(y-w)^{q-1}$ for $w \in \mathbb{F}_q$. The roots are distinct. The splitting field over $\mathbb{F}_p(b)$ is $\mathbb{F}_q(y)$. If $\sigma \in \text{Gal}(f/\mathbb{F}_p(b))$ then there is a unique $\gamma \in \text{PGL}_2(q)$ such that $\sigma(y) = \gamma^{-1}(y)$. We have $\sigma(r_w) = r_{\gamma(\sigma w)}$, where γ has the usual action by linear fractional transformations on $\mathbb{P}^1(q)$. For any $\gamma \in \text{PGL}_2(\mathbb{F}_q)$ we have*

$$\gamma^{-1}y = \frac{r_{\gamma(1)} - r_{\gamma(\infty)}}{r_{\gamma(1)} - r_{\gamma(0)}}. \quad (11)$$

Proof. All the above results were proved in [5] except for (11), which we will prove here. First, we show it in a few special cases. As above, let $y = (r_1 - r)/(r_1 - r_0)$.

- If $\gamma = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ then

$$\frac{r_{\gamma(1)} - r_{\gamma(\infty)}}{r_{\gamma(1)} - r_{\gamma(0)}} = \frac{r_1 - r_0}{r_1 - r_\infty} = 1/y = \gamma^{-1}y.$$

- If $\gamma = \begin{pmatrix} w & 0 \\ 0 & 1 \end{pmatrix}$ with $w \in \mathbb{F}_q^\times$ then

$$\begin{aligned} \frac{r_{\gamma(1)} - r_{\gamma(\infty)}}{r_{\gamma(1)} - r_{\gamma(0)}} &= \frac{r_w - r_\infty}{r_w - r_0} \\ &= \frac{r(y-w)^{q-1} - r}{r(y-w)^{q-1} - ry^{q-1}} \times \frac{y-w}{y-w} \\ &= \frac{(y-w)^q - (y-w)}{(y-w)^q - y^{q-1}(y-w)} \\ &= \frac{y^q - y}{-w + wy^{q-1}} = y/w = \gamma^{-1}y. \end{aligned}$$

- If $\gamma = \begin{pmatrix} 1 & w \\ 0 & 1 \end{pmatrix}$ with $w \in \mathbb{F}_q$, then

$$\begin{aligned}
\frac{r_{\gamma(1)} - r_{\gamma(\infty)}}{r_{\gamma(1)} - r_{\gamma(0)}} &= \frac{r_{1+w} - r_{\infty}}{r_{1+w} - r_w} \\
&= \frac{r(y-w-1)^{q-1} - r}{r(y-w-1)^{q-1} - r(y-w)^{q-1}} \times \frac{y-w-1}{y-w-1} \\
&= \frac{(y-w-1)^q - (y-w-1)}{(y-w-1)^q - (y-w)^{q-1}(y-w-1)} \\
&= \frac{y^q - y}{(y-w)^q - 1 - (y-w)^q + (y-w)^{q-1}} \times \frac{y-w}{y-w} \\
&= \frac{(y^q - y)(y-w)}{-(y-w) + (y-w)^q} \\
&= \frac{(y^q - y)(y-w)}{y^q - y} = y - w = \gamma^{-1}y.
\end{aligned}$$

Since the above three matrices generate $\text{PGL}_2(\mathbb{F}_q)$, to complete the proof we need only show that if (11) is true for γ and δ then it is true for $\gamma\delta$. Define $s_w = r_{\gamma w}$. Since (11) is true for γ , we have

$$\gamma^{-1}y = \frac{s_1 - s_{\infty}}{s_1 - s_0}.$$

Since (11) is true for δ , we have

$$\delta^{-1}(\gamma^{-1}y) = \frac{s_{\delta 1} - s_{\delta \infty}}{s_{\delta 1} - s_{\delta 0}}.$$

The left side is $(\gamma\delta)^{-1}y$. Since $s_w = r_{\gamma w}$ for all $w \in \mathbb{P}^1(\mathbb{F}_q)$, the right side is

$$\frac{r_{\gamma\delta 1} - r_{\gamma\delta \infty}}{r_{\gamma\delta 1} - r_{\gamma\delta 0}}.$$

This shows that (11) is true for $\gamma\delta$ and completes the proof. \blacksquare

Remark. If $w \in \mathbb{F}_q$, then w can explicitly be expressed in terms of the roots of $x^{q+1} - bx + b$ as follows. Let $\gamma = \begin{pmatrix} 1 & w \\ 0 & 1 \end{pmatrix}$. Then

$$\begin{aligned}
w &= y - (y - w) = y - \gamma^{-1}y \\
&= \frac{r_1 - r_{\infty}}{r_1 - r_0} - \frac{r_{\gamma 1} - r_{\gamma \infty}}{r_{\gamma 1} - r_{\gamma 0}} \\
&= \frac{r_1 - r_{\infty}}{r_1 - r_0} - \frac{r_{w+1} - r}{r_{w+1} - r_w}.
\end{aligned}$$

Proposition 3.3 *Let p be any prime (even or odd) and $q = p^n$, let F be a field of characteristic p (not necessarily perfect), and $0 \neq b \in F$. Then $x^{q+1} - bx + b$ and $x^{q+1} - x + 1/b$ have the same splitting field over F . Also, the polynomials $x^{q+1} - b^{p^i}x + b^{p^i}$ have the same splitting field over F for all $i \geq 0$.*

Proof. We begin by proving that $x^{q+1} - bx + b$ and $x^{q+1} - b^p x + b^p$ have the same splitting field over F . Denote these splitting fields by L and L_1 , respectively. Let r, r_0, r_1 be distinct roots of $x^{q+1} - bx + b$, and let $y = (r_1 - r)/(r_1 - r_0)$. Then r^p, r_0^p, r_1^p are distinct roots of $x^{q+1} - b^p x + b^p$, and $y^p = (r_1^p - r^p)/(r_1^p - r_0^p)$. By Theorem 3.1,

$$L = F \circ \mathbb{F}_q(y), \quad L_1 = F \circ \mathbb{F}_q(y^p).$$

To prove equality of these fields, it will suffice to show that

$$F_q(b, y) = \mathbb{F}_q(b, y^p),$$

or equivalently, that $y \in \mathbb{F}_q(b, y^p)$. First we express b in terms of y , using formulas from Theorem 3.1:

$$\begin{aligned} b &= r^{q+1}/(r-1) && (\text{since } r^{q+1} - br + b = 0) \\ &= (1 + \xi^{1-q})^{q+1} \xi^{q-1} && (\text{since } \xi^{q-1} = 1/(r-1)) \\ &= (1 + \xi^{1-q})^q (\xi^{q-1} + 1), \end{aligned}$$

where $\xi = y^q - y$. Noting that $\xi^q \in \mathbb{F}_q(b, y^p)$, we see that

$$\xi^{q-1} + 1 = b (1 + \xi^{q(1-q)})^{-1} \in \mathbb{F}_q(b, y^p).$$

Subtracting one from both sides, taking the reciprocal, and then multiplying by ξ^q shows that $\xi \in \mathbb{F}_q(b, y^p)$. Finally, since $\xi = y^q - y$, we conclude that $y = y^q - \xi \in \mathbb{F}_q(b, y^p)$ as required.

We showed that $x^{q+1} - b^p x + b^p$ has the same splitting field over F as $x^{q+1} - bx + b$. Repeating the argument with b^p in place of b , we see that $x^{q+1} - b^{p^2} x + b^{p^2}$ has the same splitting field over F as $x^{q+1} - b^p x + b^p$. By induction on i , all fields $x^{q+1} - b^{p^i} x + b^{p^i}$ have the same splitting field over F .

It remains to prove that $x^{q+1} - x + 1/b$ has the same splitting field as well. If r is a root of $x^{q+1} - x + 1/b$, then br is a root of $x^{q+1} - b^q x + b^q$, because

$$(br)^{q+1} - b^q(br) + b^q = b^{q+1}(r^{q+1} - r + 1/b) = 0.$$

This shows $\text{SF}(x^{q+1} - x + 1/b; F) = \text{SF}(x^{q+1} - b^q x + b^q; F)$. \blacksquare

4. Expressing roots of $C(x) + a$ in terms of $\text{SF}(x^{q+1} + ax + a; F)$

Now we apply the theory from Section 3 to derive formulas expressing the roots of $C(x) + a$ in terms of the roots of $x^{q+1} + ax + a$, where $0 \neq a \in F$. For the remainder of this article, we are working in characteristic 2; in particular $q = 2^n > 2$.

Let $e, u \in \overline{F}$ satisfy

$$C(e) = a, \quad 1/e = \langle u^{q+1} \rangle.$$

Proposition 2.6 showed that the roots of $x^{q+1} + a^2 x + a^2$ are

$$\{ \lambda \langle \zeta u \rangle^{q-1} : \zeta \in \mu_{q+1} \}, \quad \text{where } \lambda = e T(e)^2.$$

Let r, r_0, r_1 be any three distinct roots of $x^{q+1} + ax + a$. Then r^2, r_0^2, r_1^2 are distinct roots of $x^{q+1} + a^2 x + a^2$. After rescaling u by an element of μ_{q+1} , we can

arrange that $r^2 = \lambda \langle u \rangle^{q-1}$, while still keeping the condition $1/e = \langle u^{q+1} \rangle$. Next, there are $\zeta, \rho \in \mu_{q+1} \setminus \{1\}$ such that

$$r^2 = \lambda \langle u \rangle^{q-1} \quad r_0^2 = \lambda \langle \zeta^2 u \rangle^{q-1} \quad r_1^2 = \lambda \langle \rho^2 u \rangle^{q-1}.$$

Let

$$y = (r_1 - r)/(r_1 - r_0).$$

By Theorem 3.1, the splitting field of $x^{q+1} + ax + a$ is $L = F \circ \mathbb{F}_q[y]$.

Lemma 4.1 *Let y, e, ζ, ρ be as above, and let*

$$c = \frac{\langle \zeta/\rho \rangle}{\langle \zeta \rangle \langle \rho \rangle} \quad \text{and} \quad d = \frac{1}{\langle \zeta \rangle}. \quad (12)$$

The following formulas hold.

$$y^2 = \frac{\langle \rho^2 \rangle \langle \zeta^2 u \rangle}{\langle \zeta^2/\rho^2 \rangle \langle u \rangle} \quad (13)$$

$$y = \frac{\langle \rho \rangle (\zeta u + 1/\zeta)}{\langle \zeta/\rho \rangle (u + 1)} \quad (14)$$

$$u = \frac{\langle \zeta/\rho \rangle y + \langle \rho \rangle/\zeta}{\langle \zeta/\rho \rangle y + \langle \rho \rangle \zeta} \quad (15)$$

$$\langle u \rangle = \frac{1}{(cy)^2 + cy + d^2} \quad (16)$$

$$1/e = D_{q+1} \left(\frac{1}{(cy)^2 + cy + d^2} \right) \quad (17)$$

$$(y^q + y)^2 = \frac{\langle u^{q+1} \rangle}{c^2 \langle u \rangle^{q+1}} \quad (18)$$

$$e = \left(cy^2 + y + \frac{d^2}{c} \right)^{q+1} \cdot (y^q + y)^{-2}. \quad (19)$$

Proof.

$$\begin{aligned} y^2 &= \frac{r_1^2 - r^2}{r_1^2 - r_0^2} \\ &= \frac{\langle \rho^2 u \rangle^{q-1} - \langle u \rangle^{q-1}}{\langle \rho^2 u \rangle^{q-1} - \langle \zeta^2 u \rangle^{q-1}} \times \frac{\langle u \rangle \langle \rho^2 u \rangle \langle \zeta^2 u \rangle}{\langle u \rangle \langle \rho^2 u \rangle \langle \zeta^2 u \rangle} \\ &= \frac{\langle \rho^2 u \rangle^q \langle u \rangle + \langle u \rangle^q \langle \rho^2 u \rangle}{\langle \rho^2 u \rangle^q \langle \zeta^2 u \rangle + \langle \zeta^2 u \rangle^q \langle \rho^2 u \rangle} \times \frac{\langle \zeta^2 u \rangle}{\langle u \rangle} \\ &= \frac{\langle \rho^{-2} u^q \rangle \langle u \rangle + \langle u^q \rangle \langle \rho^2 u \rangle}{\langle \rho^{-2} u^q \rangle \langle \zeta^2 u \rangle + \langle \zeta^{-2} u^q \rangle \langle \rho^2 u \rangle} \times \frac{\langle \zeta^2 u \rangle}{\langle u \rangle}. \end{aligned}$$

In the first fraction, the numerator and denominator can be rewritten as follows:

$$\begin{aligned}\langle \rho^{-2}u^q \rangle \langle u \rangle + \langle u^q \rangle \langle \rho^2u \rangle &= (\rho^{-2}u^q + \rho^2u^{-q})(u + 1/u) + (u^q + u^{-q})(\rho^2u + \rho^{-2}u^{-1}) \\ &= \langle \rho^2 \rangle \langle u^{q+1} \rangle; \\ \langle \rho^{-2}u^q \rangle \langle \zeta^2u \rangle + \langle \zeta^{-2}u^q \rangle \langle \rho^2u \rangle &= \langle \zeta^2/\rho^2 \rangle \langle u^{q+1} \rangle.\end{aligned}$$

After canceling $\langle u^{q+1} \rangle$, we obtain the formula (13). To obtain (14), multiply the right side of (13) by u/u and then take the square root. Now (14) shows that u and y are related by a linear fractional transformation over \mathbb{F}_{q^2} . Solving for u in terms of y gives (15). To derive (16), let $A = \langle \zeta/\rho \rangle y + \langle \rho \rangle/\zeta$, $B = \langle \zeta/\rho \rangle y + \langle \rho \rangle \zeta$, so $u = A/B$. Then $\langle u \rangle = A/B + B/A = (A^2 + B^2)/(AB)$. It is easy to compute that $A^2 + B^2 = \langle \rho^2 \rangle \langle \zeta^2 \rangle$ and $AB = \langle \zeta/\rho \rangle^2 y^2 + \langle \zeta/\rho \rangle \langle \zeta \rangle \langle \rho \rangle y + \langle \rho \rangle^2$, and formula (16) follows. We have $1/e = \langle u^{q+1} \rangle = D_{q+1}(\langle u \rangle)$, which proves (17). For (18), we have

$$y = w \frac{\zeta u + 1/\zeta}{u + 1}, \quad y^q = w \frac{\zeta^{-1}u^q + \zeta}{u^q + 1},$$

where $w = \langle \rho \rangle / \langle \zeta/\rho \rangle \in \mathbb{F}_q$. Thus,

$$\begin{aligned}y^q + y &= w \cdot \frac{(\zeta u + 1/\zeta)(u^q + 1) + (\zeta^{-1}u^q + \zeta)(u + 1)}{(u^q + 1)(u + 1)} \\ &= \frac{w \langle \zeta \rangle (u^{q+1} + 1)}{(u + 1)^{q+1}} = \frac{(u^{q+1} + 1)}{c(u + 1)^{q+1}},\end{aligned}$$

where c is defined in (12). Now square both sides and multiply on the right by $u^{-(q+1)}/u^{-(q+1)}$ to obtain (18). Finally, (19) is obtained by substituting $1/e = \langle u^{q+1} \rangle$ and $1/\langle u \rangle = c^2 y^2 + cy + d^2$ into (18). ■

On account of Lemma 4.1, Figure 3 can be extended to incorporate other subfields of the splitting field, as shown in Figure 4.

We will need the following lemma that distinguishes the elements $1/\langle \zeta \rangle$ for $\zeta \in \mu_{q+1} \setminus \{1\}$.

Lemma 4.2 *Let $\mathbb{F}_{q,1}$ denote the elements of \mathbb{F}_q having absolute trace 1. Then*

$$\{1/\langle \zeta \rangle : \zeta \in \mu_{q+1}, \zeta \neq 1\} = \mathbb{F}_{q,1}.$$

Proof. If $a \in \mathbb{F}_q^\times$, then $x^2 + ax + 1$ has a root $r \in \mathbb{F}_q^\times$ if and only if $1/a^2 = (r/a)^2 + (r/a)$. Thus, $x^2 + ax + 1$ is reducible if and only if $\text{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(1/a) = 0$. Since $\zeta \notin \mathbb{F}_q$, its minimal polynomial $x^2 + \langle \zeta \rangle x + 1$ is irreducible, and therefore $\text{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(1/\langle \zeta \rangle) = 1$, i.e. $1/\langle \zeta \rangle \in \mathbb{F}_{q,1}$. There are exactly $q/2$ elements of $\mathbb{F}_{q,1}$ and exactly $q/2$ elements $1/\langle \zeta \rangle$, so the two sets coincide. ■

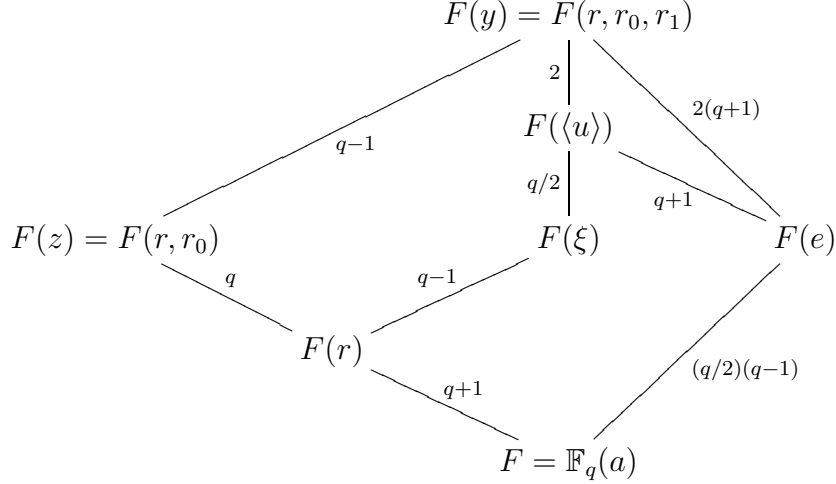


Figure 2: Joint splitting field of $x^{q+1} + ax + a$ and $C(x) + a$ when $F = \mathbb{F}_q(a)$ and a is transcendental. Here r, r_0, r_1 are any distinct roots of $x^{q+1} + ax + a$ and e is an arbitrary root of $C(x) + a$. As before, $y = (r_1 - r)/(r_1 - r_0)$, $z = r_0/r = y^{q-1}$, $\xi = y^q - y$, and $\xi^{q-1} = z(z-1)^{q-1} = 1/(r-1)$. The formulas from Lemma 4.1 show that the minimal polynomial for y over $F(\langle u \rangle)$ is $(cy)^2 + cy + d^2 - \langle u \rangle^{-1}$, where $c \in \mathbb{F}_q^\times$ and $d \in \mathbb{F}_{q,1}$ depend upon the choice of the root of $C(x)$. The minimal polynomial for $\langle u \rangle$ over $F(e)$ is $D_{q+1}(\langle u \rangle) - 1/e$. The minimal polynomial for y over $F(e)$ is $(cy^2 + y + d^2/c)^{q+1} + e(y^q + y)^2$.

Theorem 4.3 *Let $y = (r_1 - r)/(r_1 - r_0)$, where r, r_0, r_1 are three distinct roots of $x^{q+1} + ax + a$. Then the distinct roots of $C(x) + a$ are*

$$\begin{aligned} \mathcal{E} &= \left\{ D_{q+1} \left(\frac{1}{c^2 y^2 + cy + j} \right)^{-1} : c \in \mathbb{F}_q^\times, j \in \mathbb{F}_{q,1} \right\} \\ &= \left\{ \frac{(cy^2 + y + j/c)^{q+1}}{(y^q + y)^2} : c \in \mathbb{F}_q^\times, j \in \mathbb{F}_{q,1} \right\}. \end{aligned}$$

If X is an indeterminate then

$$\prod_{c \in \mathbb{F}_q^\times, j \in \mathbb{F}_{q,1}} \left(X - \frac{(cy^2 + y + j/c)^{q+1}}{(y^q + y)^2} \right) = C(X) + a. \quad (20)$$

Proof. By Lemma 4.1, if $C(e) = a$ then we can write $1/e = D_{q+1}(1/((cy)^2 + cy + j))$, where $c = \langle \zeta/\rho \rangle / (\langle \zeta \rangle \langle \rho \rangle)$ and $j = 1/\langle \zeta^2 \rangle$, and $1, \zeta, \rho$ are distinct elements of μ_{q+1} . By Lemma 4.2, $j \in \mathbb{F}_{q,1}$. There are $(q-1)$ choices for c and $q/2$ choices for j , giving a total of $(q/2)(q-1)$ pairs. This is exactly the degree of C . Since C has distinct roots, each pair (c, j) must occur. The last sentence follows from formula (19), combined with

$$C(X) + a = \prod_{e \in \mathcal{E}} (X - e).$$

■

Corollary 4.4 *The following identity holds for all y :*

$$\prod_{c \in \mathbb{F}_q^\times, j \in \mathbb{F}_{q,1}} (cy^2 + y + j/c) = 1 + (y^q + y)^{q-1}.$$

Proof. We express a in two ways. First, if we substitute $X = 0$ into (20), we obtain

$$\prod_{c \in \mathbb{F}_q^\times, j \in \mathbb{F}_{q,1}} \frac{(cy^2 + y + j/c)^{q+1}}{(y^q + y)^2} = a. \quad (21)$$

Second, by Theorem 3.1 $\xi = y^q - y$, $\xi^{q-1} = 1/(r+1)$, and $r^{q+1} + ar + a = 0$. Hence,

$$a = \frac{r^{q+1}}{r+1} = r^{q+1}\xi^{q-1} = (1 + \xi^{1-q})^{q+1}\xi^{q-1}, \quad \text{where } \xi = y^q - y.$$

Comparing the two expressions, we find that

$$\frac{\prod_{c \in \mathbb{F}_q^\times, j \in \mathbb{F}_{q,1}} (cy^2 + y + j/c)^{q+1}}{\xi^{q(q-1)}} = r^{q+1}\xi^{q-1}.$$

If a (and hence also y) is transcendental, then this may be interpreted as an identity in the ring $\mathbb{F}_q(y)$. On multiplying through by $\xi^{q(q-1)}$ and then taking the unique $(q+1)$ th root belonging to $\mathbb{F}_q(y)$, we obtain:

$$\prod_{c \in \mathbb{F}_q^\times, j \in \mathbb{F}_{q,1}} (cy^2 + y + j/c) = \xi^{q-1}r = \xi^{q-1}(1 + \xi^{1-q}) = 1 + \xi^{q-1} = 1 + (y^q + y)^{q-1}.$$

■

5. Equality of splitting fields

In this section, we prove one of our main results, that $x^{q+1} + x - 1/a$ and $C(x) + a$ have the same splitting field. This will be accomplished by explicitly writing the roots of each polynomial in terms of the roots of the other.

From here on, let

$$\mathcal{Y} = \left\{ \frac{r_1 - r}{r_1 - r_0} : r, r_0, r_1 \text{ are distinct roots of } x^{q+1} + ax + x \right\}.$$

Note that if $y \in \mathcal{Y}$ and $\gamma \in \text{PGL}_2(\mathbb{F}_q)$, then $\gamma^{-1}(y) \in \mathcal{Y}$ by (11). For $y \in \mathcal{Y}$, $c \in \mathbb{F}_q^\times$ and $j \in \mathbb{F}_{q,1}$, define

$$e(y, c, j) = \frac{(cy^2 + y + j/c)^{q+1}}{(y^q - y)^2}. \quad (22)$$

By Theorem 4.3, for a fixed y , the values $\{e(y, c, j) : c \in \mathbb{F}_q^\times, j \in \mathbb{F}_{q,1}\}$ are the distinct roots of $C(x) + a$.

Theorem 5.1 *For $q = 2^n \geq 4$, we have $\text{SF}(C(x) + a; F) = \text{SF}(x^{q+1} + x + 1/a; F) = \text{SF}(x^{q+1} + ax + a; F)$.*

Proof. The equality $\text{SF}(x^{q+1} + x + 1/a; F) = \text{SF}(x^{q+1} + ax + a; F)$ was shown in Proposition 3.3, so it suffices to show that $K = L$, where

$$K = \text{SF}(C(x) + a; F), \quad L = \text{SF}(x^{q+1} + ax + a; F).$$

Theorem 4.3 explicitly expresses each root of $C(x) + a$ in terms of the roots of $x^{q+1} + ax + a$. (See the remark following Theorem 3.1 to see how c, j can be written in terms of roots of $x^{q+1} + ax + a$.) This implies that $K \subset L$. To show $L \subset K$, we will express an arbitrary root of $x^{q+1} + ax + a$ in terms of the roots of $C(x) + a$.

Let r be an arbitrary root of $x^{q+1} + ax + a$. Select any other two roots r_0 and r_1 and define $y = (r_1 - r)/(r_1 - r_0)$, $\xi = y^q - y$. By Theorem 3.1, $r = 1 + \xi^{1-q}$, so it suffices to express ξ in terms of the roots of $C(x) + a$. By Theorem 4.3, these roots are $\{e(y, c, j) : c \in \mathbb{F}_q, j \in \mathbb{F}_{q,1}\}$, where $e(y, c, j) = (cy^2 + y + j/c)^{q+1}/\xi^2$.

First assume that $q > 4$. We have

$$\begin{aligned} e(y, c, j) &= (cy^{2q} + y^q + j/c)(cy^2 + y + j/c)/\xi^2 \\ &= \frac{c^2y^{2q+2} + c(y^{2q+1} + y^{q+2}) + y^{q+1} + j\xi^2 + (j/c)\xi + (j/c)^2}{\xi^2}. \end{aligned}$$

We claim that there are $c_1, c_2, c_3, c_4 \in \mathbb{F}_q^\times$ such that $\sum_{i=1}^4 c_i = 1$ and $\sum_{i=1}^4 1/c_i = 0$. To see this, select $\alpha \in \mathbb{F}_q \setminus \mathbb{F}_4$; such α exists because $q > 4$. Let $w_1 = 1$, $w_2 = \alpha$, $w_3 = 1/\alpha$, and note that $w_1 + w_2 + w_3 = 1 + \alpha + \alpha^{-1} = 1/w_1 + 1/w_2 + 1/w_3$. Furthermore, this value does not belong to \mathbb{F}_2 , because the only solutions to $x + 1/x + 1 \in \{0, 1\}$ belong to \mathbb{F}_4 . Set $w_4 = 1/(1 + \alpha + \alpha^{-1})$. Then $1/w_1 + 1/w_2 + 1/w_3 + 1/w_4 = 0$. Since $w_4 \notin \mathbb{F}_2$, we know $w_4 \neq w_4^{-1}$, and so $w_1 + w_2 + w_3 + w_4 = 1 + \alpha + \alpha^{-1} + w_4 = 1/w_4 + w_4 \neq 0$. Setting $c_i = w_i / \sum w_i$, we find that $\sum c_i = 1$ and $\sum c_i^{-1} = 0$. This establishes the claim. Let

$$\begin{aligned} t_1(c, j) &= \sum_{i=1}^4 e(y, cc_i, j) = \frac{c^2y^{2q+2} + c(y^{2q+1} + y^{q+2})}{\xi^2}, \\ t_2(c, j) &= e(y, c, j) - t_1(c, j) = \frac{y^{q+1} + j\xi^2 + (j/c)\xi + (j/c)^2}{\xi^2} \end{aligned}$$

and note that these both belong to K . Since $t_1(c, j)$ does not depend on j , we may denote it simply $t_1(c)$. For any $j_1, j_2 \in \mathbb{F}_{q,1}$ we have

$$t_2(j_1, j_1) + t_2(j_2, j_2) = j_1 + j_2 \in K.$$

Note that $j_1 + j_2$ represents an arbitrary element of $\mathbb{F}_{q,0}$. In addition, we have for any $j \in \mathbb{F}_{q,1}$ and $b \in F \setminus \mathbb{F}_2$:

$$t_2(j, j) + t_2(j/(b+1), j) = \frac{b}{\xi} + \frac{b^2}{\xi^2} \in K. \quad (23)$$

Also,

$$t_2(j/(b+1), j) + t_2(j/b, j) = \frac{1}{\xi} + \frac{1}{\xi^2} \in K.$$

Combining this with (23), we see that in fact $b/\xi + b^2/\xi^2 \in K$ for all $b \in \mathbb{F}_q$.

Next we show that $\xi \in K$. Select distinct values $d_1, d_2, d_3 \in \mathbb{F}_{q,1}$ such that $d_i + d_j \neq 1$ for each i, j . To see that these exist, note that if n is odd, then $1 \in \mathbb{F}_{q,1}$, and so the sum of two elements of $\mathbb{F}_{q,1}$ is never one and it suffices to select d_1, d_2, d_3 to be distinct. Since $|\mathbb{F}_{q,1}| = q/2 \geq 4$, this selection is possible. If n is even, then $q/2 \geq 8$, so there are at least eight choices for $d_1 \in \mathbb{F}_{q,1}$, six choices for $d_2 \in \mathbb{F}_{q,1} \setminus \{d_1, d_1 + 1\}$, and four choices for $d_3 \in \mathbb{F}_{q,1} \setminus \{d_1, d_2, d_1 + 1, d_2 + 1\}$. This shows again that d_1, d_2, d_3 can be selected so that $d_i + d_j \neq 1$ for each pair (i, j) . Let $\tau_1 = d_1 + d_2$ and $\tau_2 = d_1 + d_3$, and note that $\{\tau_1, \tau_2, \tau_1 + \tau_2\} \cap \mathbb{F}_2 = \emptyset$. Let

$$c_1 = \frac{1}{\tau_1(\tau_1 + \tau_2)}, \quad c_2 = \frac{1}{\tau_2(\tau_1 + \tau_2)}$$

and observe that

$$\tau_1 c_1 + \tau_2 c_2 = 0, \quad \tau_1^2 c_1 + \tau_2^2 c_2 = 1.$$

Since τ_i and $c_i/\xi + c_i^2/\xi^2$ are in K , so is

$$\tau_1^2(c_1/\xi + c_1^2/\xi^2) + \tau_2^2(c_2/\xi + c_2^2/\xi^2) = 1/\xi.$$

This shows $\xi \in K$, so $r \in K$. Since r is an arbitrary root of $x^{q+1} + ax + b$, this completes the proof when $q > 4$.

If $q = 4$, then let α be a cube root of unity in \mathbb{F}_4 . By direct calculation,

$$1/\xi = e(y, 1, \alpha) + e(y, 1, \alpha^2) + \frac{(e(y, \alpha, \alpha) + e(y, \alpha, \alpha^2))(e(y, \alpha^2, \alpha) + e(y, \alpha^2, \alpha^2))}{e(y, 1, \alpha) + e(y, 1, \alpha^2)}.$$

Thus, $\xi \in K$ and consequently $r \in K$, as desired. \blacksquare

6. Galois action and related factorizations

Since the roots of the two polynomials $C(x) + a$ and $x^{q+1} + ax + a$ belong to the same field $L = F \circ \mathbb{F}_q(y)$, any element of the Galois group $\text{Gal}(L/F)$ simultaneously permutes the roots of $C(x) + a$ and of $x^{q+1} + ax + a$. For this reason, the factorizations of these two polynomials are related. This section explores this.

We recall from Section 3 that an ordered triple (r, r_0, r_1) of distinct roots of $x^{q+1} + ax + a$ determines $y = (r_1 - r)/(r_1 - r_0)$. If we selected a different triple of roots, then the cross-ratio y' that they determine satisfies $y' = \gamma^{-1}y$ for a unique $\gamma \in \text{PGL}_2(\mathbb{F}_q)$. It will be useful to see the effect of such transformations on the roots of $C(x) + a$.

Recall that the distinct roots of $C(x) + a$ are $\{e(y, c, j) : c \in \mathbb{F}_q^\times, j \in \mathbb{F}_{q,1}\}$, where $e(y, c, j) = (cy^2 + y + j/c)^{q+1}/(y^q + y)^2$.

Lemma 6.1 *If $b \in \mathbb{F}_q^\times$ then*

$$e(y + b, c, j) = e(y, c, j + bc + (bc)^2) \tag{24}$$

$$e(by, c, j) = e(y, bc, j) \tag{25}$$

$$e(1/y, c, j) = e(y, j/c, j) \tag{26}$$

Proof. For the first formula, $(y+b)^q - (y+b) = y^q - y$ and $c(y+b)^2 + (y+b) + j/c = cy^2 + y + (j + cb + c^2b^2)/c$. Note that $j + cb + c^2b^2 \in \mathbb{F}_{q,1}$, because

$$\text{Tr}(j + bc + b^2c^2) = \text{Tr}(j) + 2\text{Tr}(bc) = \text{Tr}(j) = 1,$$

where Tr denotes the trace from \mathbb{F}_q to \mathbb{F}_2 . For the second formula,

$$e(by, c, j) = \frac{(cb^2y^2 + by + j/c)^{q+1}}{((by)^q + by)^2} = \frac{b^{q+1}(cb^2y^2 + y + j/(cb))^{q+1}}{b^2(y^q + y)^2} = e(y, bc, j).$$

Finally,

$$e(1/y, c, j) = \frac{(cy^{-2} + y^{-1} + j/c)^{q+1}}{(y^{-q} + y^{-1})^2} \times \frac{y^{2(q+1)}}{y^{2(q+1)}} = \frac{(c + y + (j/c)y^2)^{q+1}}{(y + y^q)^2} = e(y, j/c, j).$$

■

Theorem 6.2 *Let L be the splitting field of $x^{q+1} + x + 1/a$ (which is also the splitting field of $C(x) + a$ by Theorem 5.1), and let $\sigma \in \text{Gal}(L/F \circ \mathbb{F}_q)$.*

- (i) *If σ fixes at least three roots of $x^{q+1} + x + 1/a$, then it fixes all roots of $x^{q+1} + x + 1/a$ and all roots of $C(x) + a$.*
- (ii) *If σ fixes exactly two roots of $x^{q+1} + x + 1/a$, then the permutation induced by σ on the roots has orbits of size $[1, 1, \delta, \delta, \dots, \delta]$ where δ divides $q-1$. The permutation induced by σ on the roots of $C(x) + a$ has all its orbits of size δ .*
- (iii) *If σ fixes exactly one root of $x^{q+1} + x + 1/a$, then the remaining roots fall into σ -orbits of size 2. Also, σ fixes exactly $q/2$ roots of $C(x) + a$, and the remaining roots fall into exactly $q/2(q/2 - 1)$ σ -orbits of size two.*
- (iv) *If σ fixes no roots of $x^{q+1} + x + 1/a$, then all σ -orbits of $x^{q+1} + x + 1/a$ have the same size δ , where δ divides $q+1$. Also, σ fixes exactly one root of $C(x) + a$, and all remaining roots belong to σ -orbits of size δ .*

Proof. Since $x^{q+1} + x + 1/a$ and $x^{q+1} + ax + a$ have the same splitting field and their roots are in bijection by a Galois-invariant map, we can instead work with $x^{q+1} + ax + a$.

In case (i), let r, r_0, r_1 be three roots of $x^{q+1} + ax + a$ that are fixed by σ . Then $y = (r_1 - r)/(r_1 - r_0)$ is also fixed by σ . By Theorem 3.1, $L = F \circ \mathbb{F}_q(y)$. Since $\sigma \in \text{Gal}(L/F \circ \mathbb{F}_q)$ and it fixes y , it follows that σ is the identity, and so it fixes all roots of both polynomials.

In case (ii), let r and r_0 be roots of $x^{q+1} + ax + a$ that are fixed by σ , and select a third root r_1 with which to form y . Let γ be the element of $\text{PGL}_2(q)$ such that $\sigma(r_w) = r_{\gamma(w)}$ and $\sigma(y) = \gamma^{-1}y$. (Such γ exists by Theorem 3.2.) Since γ fixes ∞ and 0, it must be of the form $\begin{pmatrix} b & 0 \\ 0 & 1 \end{pmatrix}$ with $b \in \mathbb{F}_q^\times$. Let δ be the multiplicative order of b . Then the orbits of γ acting on $\mathbb{P}^1(q) \setminus \{\infty, 0\}$ are of the form $\{w, bw, b^2w, \dots, b^{\delta-1}w\}$ showing that the non-singleton orbits all have the same order δ . Consequently, the σ -orbits on roots of $x^{q+1} + x + 1/a$ have sizes $[1, 1, \delta, \delta, \dots, \delta]$. The action on roots of $C(x) + a$ is

$$\sigma(e(y, c, j)) = e(by, c, j) = e(y, bc, j).$$

Thus, each σ -orbit has size exactly δ .

In case (iii), σ fixes exactly one root of $x^{q+1} + ax + a$ which we may assume is r . The elements of $\text{PGL}_2(q)$ that fix only ∞ are of the form $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ with $b \in \mathbb{F}_q^\times$. Then

$$\sigma(e(y, c, j)) = e(y + b, c, j) = e(y, c, j + (bc) + (bc)^2).$$

Since b and c are nonzero, we can have $(c, j) = (c, j + (bc) + (bc)^2)$ if and only if $c = 1/b$. So the $q/2$ roots $e(y, 1/b, j)$ are fixed, and the other roots belong to σ -orbits of size 2.

In case (iv), define y with respect to three roots r, r_0, r_1 of $x^{q+1} + ax + a$ such that $\sigma(r) = r_0$ and $\sigma(r_0) = r_1$. By Theorem 3.2, there is a unique $\gamma \in \text{PGL}_2(\mathbb{F}_q)$ such that $\sigma(y) = \gamma^{-1}(y)$ and $\sigma(r_w) = r_{\gamma(w)}$ for all $w \in \mathbb{P}^1(\mathbb{F}_q)$. Since γ takes ∞ to 0 and 0 to 1, it has the form $\gamma = \begin{pmatrix} 0 & 1 \\ k & 1 \end{pmatrix}$. By hypothesis, σ fixes no roots, and so $1/(kw + 1) = w$ has no solutions in \mathbb{F}_q . This is equivalent to $(kw)^2 + (kw) + 1$ having no rational roots, which is equivalent to $k \in \mathbb{F}_{q,1}$. Let δ be the order of γ . We will show in Proposition 7.1 (or see [3]) that δ divides $q + 1$ and that γ has no fixed points in $\mathbb{P}^1(\mathbb{F}_q)$. (In the notation of (29), γ belongs to the group $\mathcal{C}_{\sqrt{k}, \sqrt{k}}$, which is cyclic of order $q + 1$.) Thus, the orbits of σ on the roots of $x^{q+1} + ax + a$ all have the same size, δ .

We have $\gamma^{-1}y = (1/y + 1)/k$, and so

$$\begin{aligned} \sigma(e(y, c, j)) &= e((1/y + 1)/k, c, j) \\ &= e(1/y + 1, c/k, j) \quad \text{by (25)} \\ &= e(1/y, c/k, j + c/k + c^2/k^2) \quad \text{by (24)} \\ &= e(y, jk/c + 1 + c/k, j + c/k + c^2/k^2) \quad \text{by (26)}. \end{aligned}$$

This can equal $e(y, c, j)$ only if $(c/k) + (c/k)^2 = 0$, i.e. $c = k$. In that case, we have

$$\sigma(e(y, k, j)) = e(y, j, j).$$

So, for the root to be fixed by σ we also need $j = k$. Thus, we find there is exactly one fixed root, namely $e(y, j, j)$. The other roots must belong to orbits of size dividing δ , where δ is the order of γ . We claim the orbits have size exactly δ . Indeed, suppose that σ had an orbit of size i , where i strictly divides δ , and consider σ^i . This fixes no roots of $x^{q+1} + ax + a$, so it fixes exactly one root of $C(x) + a$, which must be $e(y, j, j)$. But it also fixes the points on the σ -orbit of size i , a contradiction. So the roots of $C(x) + a$ fall into σ -orbits of size $[1, \delta, \delta, \dots, \delta]$. ■

Corollary 6.3 *For a polynomial $g \in F[x]$, write $g \sim [n_1, n_2, \dots, n_t]$ if g factors into irreducibles of degrees n_1, n_2, \dots, n_t . Let $0 \neq a \in F = \mathbb{F}_{q^m}$, where $q = 2^n > 2$. Let $f(x) = x^{q+1} + x$ and let $C(x) = xT(x)^{q+1}$.*

- (i) *If $f(x) + 1/a$ has at least three roots in F then both $f(x) + 1/a$ and $C(x) + a$ have all their roots in F .*
- (ii) *If $f(x) + 1/a$ has exactly two roots in F , then $f(x) + 1/a \sim [1, 1, \dots, 1]$ and $C(x) + a \sim [1, \dots, 1]$, where $\vdash q - 1$.*
- (iii) *If $f(x) + 1/a$ has exactly one root in F then $f(x) + 1/a \sim [1, 2, 2, \dots, 2]$ and $C(x) + a \sim [1, 1, \dots, 1, 2, 2, \dots, 2]$, where $C(x) + a$ has $q/2$ linear factors and $(q^2 - 2q)/4$ irreducible quadratic factors.*

(iv) If $f(x) + 1/a$ has no roots in F , then $f(x) + 1/a \sim [\cdot, \cdot, \dots, \cdot]$ and $C(x) + a \sim [1, \cdot, \cdot, \dots, \cdot]$, where $\cdot = q + 1$.

Proof. Apply Theorem 6.2, taking σ to be the Frobenius map: $\sigma(u) = u^{|F|}$. The sizes of the σ -orbits acting on the roots of $f(x) + 1/a$ or $C(x) + a$ are the degrees of the irreducible factors over F . ■

Corollary 6.4 If $F = \mathbb{F}_{q^m}$ and $0 \neq a \in F$ then $C(x) + a$ has exactly 0, 1, $q/2$, or $(q/2)(q-1)$ roots in F . Let c_i denote the number of $a \in F^\times$ for which $C(x) + a$ has exactly i roots in F . If m is even, then

$$c_0 = \frac{(q-2)(q^m-1)}{2(q-1)}, \quad c_1 = \frac{q^{m+1}-q}{2(q+1)}, \quad c_{q/2} = q^{m-1}, \quad c_{(q/2)(q-1)} = \frac{q^{m-1}-q}{q^2-1}.$$

If m is odd, then

$$c_0 = \frac{(q-2)(q^m-1)}{2(q-1)}, \quad c_1 = \frac{q^{m+1}+q}{2(q+1)}, \quad c_{q/2} = q^{m-1}-1, \quad c_{(q/2)(q-1)} = \frac{q^{m-1}-1}{q^2-1}.$$

Proof. For $i \in \{0, 1, 2, q+1\}$, let N_i denote the number of $a \in \mathbb{F}^\times$ such that $x^{q+1} + ax + a$ has exactly i roots. By Corollary 6.3, we have $N_0 = c_1$, $N_1 = c_{q/2}$, $N_2 = c_0$, and $N_{q+1} = c_{(q/2)(q-1)}$. The N_i 's are computed in [5, Theorem 5.6]. The result follows. ■

We conclude this section by proving Proposition 1.1, which gives the related factorizations of $x^{q+1} + x + 1/a$ and $C(x) + a$ when $q = 4$ and $F = \mathbb{F}_{2^k}$. Note that we are not assuming that $\mathbb{F}_q \subset F$. The polynomials are $x^5 + x + 1/a$ and $x(x+1)^5 + a$. Since $x^5 + ax + a$ has the same splitting field and factorization type as $x^5 + x + 1/a$, we may study it instead. Let L denote the splitting field and let $\sigma \in \text{Gal}(L/F)$ denote the Frobenius element, $\sigma(b) = b^{|F|}$; then σ generates $\text{Gal}(L/F)$.

If k is even, then $\mathbb{F}_q \subset F$. In that case, Proposition 1.1 follows from Corollary 6.3.

Now assume k is odd, and we must show that one of the following cases holds.

$$x^5 + x + 1/a \sim [1, 1, 1, 2] \text{ and } x(x+1)^5 + a \sim [2, 2, 2]$$

$$x^5 + x + 1/a \sim [1, 4] \text{ and } x(x+1)^5 + a \sim [1, 1, 4]$$

$$x^5 + x + 1/a \sim [2, 3] \text{ and } x(x+1)^5 + a \sim [6].$$

Note that $\sigma(c) = c^2$ for $c \in \mathbb{F}_4$.

If σ fixes at least three roots of $x^{q+1} + ax + a$, then we can arrange for y to be rational. Then $\sigma(r_w) = r_{\sigma(w)}$ for $w \in \mathbb{P}^1(\mathbb{F}_4)$. The conjugate pair α and α^2 are exchanged, while all other elements are fixed, and so $x^5 + ax + a \sim [1, 1, 1, 2]$. The roots of $C(x) + a$ are $e(y, c, j)$ for $c \in \{1, \alpha, \alpha^2\}$ and $j \in \{\alpha, \alpha^2\}$. Since y is fixed, we have $\sigma(e(y, c, j)) = e(y, c^2, j^2)$. There are three orbits of size 2, so $C(x) + a \sim [2, 2, 2]$.

Now suppose that σ fixes exactly one or two roots, so there is at least one rational root r . Select r_0 to be any root that is not fixed by σ , and let $r_1 = \sigma(r_0)$. Set $y = (r_1 - r)/(r_1 - r_0)$ and $r_w = r(y - w)^{q-1}$. By Theorem 3.2 there is a unique $\gamma \in \text{PGL}_2(\mathbb{F}_q)$ such that $\sigma(r_w) = r_{\gamma(w^2)}$ and $\sigma(y) = \gamma^{-1}(y)$. Let $\sigma(r_1) = r_{1+b}$, so $b \in \mathbb{F}_4^\times$.

Now $\gamma(\infty) = \infty$, $\gamma(0) = 1$, and $\gamma(1) = 1 + b$. From this we see that $\gamma = \begin{pmatrix} b & 1 \\ 0 & 1 \end{pmatrix}$. We have $\sigma(r_w) = r_{bw^2+1}$. If $b = 1$ then σ fixes ∞ , α , and α^2 , contradicting that σ fixes exactly one or two roots. Thus, $b = \alpha$ or $b = \alpha^2$. Let us assume that $b = \alpha$, as the other case is similar. Then, $\sigma(r_0) = r_1$, $\sigma(r_1) = r_{\alpha+1}$, $\sigma(r_{\alpha+1}) = r_\alpha$, and $\sigma(r_\alpha) = r_0$, thus $x^5 + ax + a \sim [1, 4]$. The action on roots of $C(x) + a$ is given by

$$\begin{aligned} \sigma(e(y, c, j)) &= e(\gamma^{-1}y, c^2, j^2) = e((y+1)/b, c^2, j^2) = e(y+1, c^2/b, j^2) \\ &= e(y, c^2/b, j^2 + c^2/b + c/b^2). \end{aligned}$$

Setting $b = \alpha$, the σ -orbits are as follows:

$$e(y, 1, \alpha) \rightarrow e(y, \alpha^2, \alpha) \rightarrow e(y, 1, \alpha^2) \rightarrow e(y, \alpha^2, \alpha^2) \rightarrow e(y, 1, \alpha)$$

while $e(y, \alpha, \alpha)$ and $e(y, \alpha, \alpha^2)$ are fixed. Thus, $C(x) + a \sim [1, 1, 4]$, as claimed.

It remains to consider the case where $x^5 + ax + a$ has no rational roots. Select three roots as follows. Let r_∞ belong to an orbit of odd order, let $r_0 = \sigma(r_\infty)$, and let $r_1 = \sigma(r_0)$. Either $\sigma(r_1) = r_\infty$ or $\sigma(r_1) = r_c$ with $c \in \{\alpha, \alpha^2\}$. Since $\sigma(r_w) = r_{\gamma\sigma(w)}$, we know γ takes $(\infty, 0, 1)$ to $(0, 1, \infty)$ or $(0, 1, c)$. In the former case, $\gamma = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$, and in the latter case, $\gamma = \begin{pmatrix} 0 & 1 \\ c & 1 \end{pmatrix}$, where $c \in \{\alpha, \alpha^2\}$. In the latter case, r_{c+1} is fixed, because $\sigma(r_{c+1}) = r_{\gamma(\sigma(c+1))} = r_{\gamma(c)} = r_{1/(c^2+1)} = r_{c+1}$. Since we were assuming no rational roots, this case can be eliminated from consideration. Thus, we have $\gamma = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$.

For $\gamma = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$, we have $\sigma(r_w) = r_{\gamma(w^2)}$, and the σ -orbits on $\{r_w : w \in \mathbb{P}^1(q)\}$ are $(\infty \ 0 \ 1)(\alpha \ \alpha + 1)$. The action on roots of $C(x) + a$ is

$$\begin{aligned} \sigma(e(y, c, j)) &= \sigma(\gamma^{-1}(y), c^2, j^2) = \sigma((1/y) + 1, c^2, j^2) = \sigma(1/y, c^2, j^2 + c^2 + c) \\ &= \sigma(y, (j^2/c^2) + 1 + 1/c, j^2 + c^2 + c) = \sigma(y, cj^2 + 1 + c^2, j^2 + c^2 + c), \end{aligned}$$

where we used $c^3 = j^3 = 1$ since $|\mathbb{F}_q^\times| = 3$. There is a single σ -orbit:

$$e(y, 1, \alpha) \rightarrow e(y, \alpha^2, \alpha^2) \rightarrow e(y, \alpha, \alpha^2) \rightarrow e(y, 1, \alpha^2) \rightarrow e(y, \alpha, \alpha) \rightarrow e(y, \alpha^2, \alpha) \rightarrow e(y, 1, \alpha).$$

So in this case, $x^5 + x + 1/a \sim [3, 2]$ and $x(x+1)^5 + a \sim [6]$.

7. Dihedral group

Let L be the splitting field of $x^{q+1} + ax + a$ and let $e \in L$ be a root of $C(x) + a$. As shown in Figure 4, when $F = \mathbb{F}_q(a)$ with a transcendental we have $[L : F(e)] = 2(q+1)$. Thus, $\text{Gal}(L/F(e))$ is a subgroup of order $2(q+1)$ in $\text{PGL}_2(\mathbb{F}_q)$, and by [3, Chapter XII], the only such subgroup is a dihedral group. In this section, we give explicit formulas for this dihedral group. Later, we will use these formulas to give a new proof that $C(x)$ is exceptional when n is odd.

First, we discuss $\text{PGL}_2(\mathbb{F}_q)$ (where $q = 2^n$) in more detail. Dickson [3, Chapter XII] showed that all nontrivial elements of $\text{PGL}_2(\mathbb{F}_q)$ have order 2, or have order dividing $q-1$, or have order dividing $q+1$. In fact, he enumerated these:

$q^2 - 1$ elements have order 2

$(q+1)(q/2)(q-2)$ elements have order dividing $q-1$

$q^2(q-1)/2$ elements have order dividing $q+1$.

Including also the trivial element, these numbers add up correctly to the full cardinality of $\text{PGL}_2(\mathbb{F}_q)$:

$$q^2 - 1 + (q+1)(q/2)(q-2) + q(q-1)(q/2) + 1 = q(q-1)(q+1).$$

We would like to explicitly describe these elements in a simple manner. If an element $\gamma \in \text{PGL}_2(\mathbb{F}_q)$ is normalized to have determinant 1, then its order divides $q+1$ if and only if it is conjugate to $\text{diag}\{\rho, \rho^{-1}\}$ with $\rho \in \mu_{q+1}$. In that case, its trace is $\langle \rho \rangle$. By Lemma 4.2, such values are characterized by the fact that $1/\langle \rho \rangle \in \mathbb{F}_{q,1}$. Thus, for any nontrivial $\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ we have

$$\text{order}(\gamma) \text{ divides } q+1 \text{ iff } A+D \neq 0 \text{ and } \text{Tr}_{\mathbb{F}_q/\mathbb{F}_2}((AD-BC)/(A^2+D^2)) = 1.$$

The order divides $q-1$ if and only if it is conjugate to $\text{diag}\{w, 1/w\}$ with $w \neq w^{-1} \in \mathbb{F}_q^\times$. In that case, $\langle w \rangle = w + 1/w$ is nonzero and $\text{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(1/\langle w \rangle) = 0$. Thus,

$$\text{order}(\gamma) \text{ divides } q-1 \text{ iff } A+D \neq 0 \text{ and } \text{Tr}_{\mathbb{F}_q/\mathbb{F}_2}((AD-BC)/(A^2+D^2)) = 0.$$

Finally, if γ has order 2 then its eigenvalues are equal, so its (matrix) trace is zero:

$$\text{order}(\gamma) = 2 \text{ iff } A = D \text{ and } B \text{ or } C \text{ is nonzero.}$$

To count the matrices of order 2, we note that if we include the identity matrix then each can be written uniquely as either $\begin{pmatrix} 1 & b \\ c & 1 \end{pmatrix}$ with $bc \neq 1$, or as $\begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix}$ with $bc = 1$, so the total number of matrices equals the number of pairs (b, c) , which is q^2 . Excluding the identity, there are exactly $q^2 - 1$ matrices of order 2.

In the remaining cases we have $A+D \neq 0$. Consider $(AD-BC)/(A+D)^2$. The absolute trace of this quantity determines whether the order of γ divides $q-1$ or $q+1$. If $BC = 0$, then the absolute trace is always zero because

$$\frac{AD}{A^2+D^2} = \frac{D}{A+D} + \left(\frac{D}{A+D} \right)^2.$$

If $BC \neq 0$, then we choose to normalize so that $BC = 1$, and we have

$$\frac{AD+1}{A^2+D^2} = \frac{D}{A+D} + \left(\frac{D}{A+D} \right)^2 + \frac{1}{(A+D)^2}.$$

Set $j = 1/(A+D) \in \mathbb{F}_q^\times$. We have proved that if

$$\gamma = \begin{pmatrix} A & 1/C \\ C & A+1/j \end{pmatrix} \in \text{PGL}_2(\mathbb{F}_q) \tag{27}$$

then the order of γ divides $q+1$ if and only if $j \in \mathbb{F}_{q,1}$, and otherwise the order of γ divides $q-1$. Note that $j^2 \det(\gamma) = j^2 A^2 + jA + j^2$. If $\text{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(j) = 1$, this has no rational solutions for A , and so we obtain a matrix for every triple $(A, C, j) \in \mathbb{F}_q \times \mathbb{F}_q^\times \times \mathbb{F}_{q,1}$. There are exactly $q(q-1)(q/2)$ such triples, which agrees with Dickson's count.

By a direct computation, we find that if $A_1 + A_2 + 1/j \neq 0$ then

$$\begin{pmatrix} A_1 & 1/C \\ C & A_1 + 1/j \end{pmatrix} \begin{pmatrix} A_2 & 1/C \\ C & A_2 + 1/j \end{pmatrix} = \begin{pmatrix} A_3 & 1/C \\ C & A_3 + 1/j \end{pmatrix}, \quad \text{where } A_3 = \frac{1 + A_1 A_2}{A_1 + A_2 + 1/j}.$$

Thus, if C, j are held fixed then the elements of the form (27), together with the identity, are closed under multiplication and so they form a group which we denote by $\mathcal{C}_{j,C}$. (Here we must exclude the matrices of determinant zero.) We may associate the identity element with “ $A = \infty$ ”.

It is useful to observe that

$$\begin{pmatrix} C & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} A & 1/C \\ C & A + 1/j \end{pmatrix} \begin{pmatrix} 1/C & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} A & 1 \\ 1 & A + 1/j \end{pmatrix} \quad (28)$$

Often this makes it easy to reduce to the case $C = 1$. We let \mathcal{C}_j denote the cyclic group consisting of matrices $M_A = \begin{pmatrix} A & 1 \\ 1 & A + 1/j \end{pmatrix}$. Note that the value j does not change under the above conjugation. This is an advantage of the normalization $BC = 1$.

Also we note the formula:

$$\begin{pmatrix} 1 & \frac{1}{jC} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} A & \frac{1}{C} \\ C & A + \frac{1}{j} \end{pmatrix} \begin{pmatrix} 1 & \frac{1}{jC} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} A & \frac{1}{C} \\ C & A + \frac{1}{j} \end{pmatrix}^{-1}.$$

Thus, the group generated by $\mathcal{C}_{j,C}$ and $\begin{pmatrix} 1 & 1/(jC) \\ 0 & 1 \end{pmatrix}$ is dihedral of order $2(q-1)$ (if $j \in \mathbb{F}_{q,0}$) or $2(q+1)$ (if $j \in \mathbb{F}_{q,1}$).

Another point is worth making. Let $\mathcal{B} \subset \text{PGL}_2(\mathbb{F}_q)$ denote the matrices that fix ∞ , i.e., matrices of the form $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$, where $a \in \mathbb{F}_q^\times$ and $b \in \mathbb{F}_q$. Suppose $j \in \mathbb{F}_{q,1}$, so \mathcal{C}_j has order $q+1$. Since $\mathcal{C}_j \cap \mathcal{B} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$, and $|\mathcal{C}_j| \cdot |\mathcal{B}| = (q+1) \cdot q(q-1) = |\text{PGL}_2(\mathbb{F}_q)|$, we see that each element of $\text{PGL}_2(\mathbb{F}_q)$ can be decomposed uniquely as $\delta\beta$ with $\delta \in \mathcal{C}_j$ and $\beta \in \mathcal{B}$. Alternatively, each element may be decomposed uniquely as $\beta\delta$.

Let $M_A \in \mathcal{C}_j$, where $j \in \mathbb{F}_{q,1}$, and suppose we wish to compute all conjugates, $\gamma^{-1}M_A\gamma$. Decompose $\gamma = \delta\beta$, where $\delta \in \mathcal{C}_j$ and $\beta \in \mathcal{B}$. Then $\gamma^{-1}M_A\gamma = \beta^{-1}M_A\beta$. We may decompose β as

$$\beta = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}.$$

Conjugating M_A by $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ gives

$$\begin{pmatrix} 1 & b \\ 1 & 0 \end{pmatrix} \begin{pmatrix} A & 1 \\ 1 & A + 1/j \end{pmatrix} \begin{pmatrix} 1 & b \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} A+b & u \\ 1 & A+b+1/j \end{pmatrix}, \quad \text{where } u = 1 + b^2 + b/j.$$

Since $\text{Tr}(uj^2) = \text{Tr}(j^2 + (bj)^2 + (bj)) = \text{Tr}(j^2)$, we see that if $j \in \mathbb{F}_{q,1}$ then $u \neq 0$. As explained above, it is useful to normalize to make the product of the off-diagonal entries equal to 1, which in this case amounts to dividing each entry by \sqrt{u} . Then

$$\begin{pmatrix} 1 & b \\ 1 & 0 \end{pmatrix} \begin{pmatrix} A & 1 \\ 1 & A + 1/j \end{pmatrix} \begin{pmatrix} 1 & b \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} (A+b)/\sqrt{u} & \sqrt{u} \\ 1/\sqrt{u} & (A+b+1/j)/\sqrt{u} \end{pmatrix} = \begin{pmatrix} A' & C \\ 1/C & A' + 1/J \end{pmatrix}$$

where

$$A' = (A+b)/(1+b+\sqrt{b/j}), \quad C = 1+b+\sqrt{b/j}, \quad J = j(1+b+\sqrt{b/j}) = j+\sqrt{bj}+bj.$$

Note that $\text{Tr}(J) = 1$, since $\text{Tr}(\sqrt{bj} + bj) = 0$. Conjugating this result by $\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$ fixes J but changes C to aC . It was pointed out by Dickson that all the cyclic subgroups of order $q+1$ are conjugate. The above formulas make this explicit.

We summarize part of our discussion in the following proposition, which shows that the dihedral groups of order $2q+2$ are naturally parameterized by $\mathbb{F}_{q,1} \times \mathbb{F}_q^\times$.

Proposition 7.1 *Let $q = 2^n$, $C \in \mathbb{F}_q^\times$, and $j \in \mathbb{F}_{q,1}$, i.e., $\text{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(j) = 1$. For $A \in \mathbb{P}^1(\mathbb{F}_q)$, define $M_A \in \text{PGL}_2(\mathbb{F}_q)$ by the formula*

$$M_A = \begin{pmatrix} A & 1/C \\ C & A+1/j \end{pmatrix} \quad \text{if } A \in \mathbb{F}_q, \quad M_\infty = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Define

$$\mathcal{C}_{j,C} = \{M_A : A \in \mathbb{P}^1(\mathbb{F}_q)\}, \quad \mathcal{D}_{j,C} = \mathcal{C}_{j,C} \cup \left\{ M_A \begin{pmatrix} 1 & \frac{1}{jC} \\ 0 & 1 \end{pmatrix} : A \in \mathbb{P}^1(\mathbb{F}_q) \right\}. \quad (29)$$

Then $\mathcal{C}_{j,C}$ is a cyclic group of order $q+1$, and $\mathcal{D}_{j,C}$ is a dihedral group of order $2(q+1)$. Any nontrivial element of this group has no fixed points in $\mathbb{P}^1(\mathbb{F}_q)$. We have

$$M_A M_B = M_K, \text{ with } K = \frac{1+AB}{1/j + A + B}, \quad (30)$$

$$\begin{pmatrix} 1 & \frac{1}{jC} \\ 0 & 1 \end{pmatrix} M_A \begin{pmatrix} 1 & \frac{1}{jC} \\ 0 & 1 \end{pmatrix} = M_A^{-1} = M_{A+1/j}. \quad (31)$$

Proof. M_A is invertible because $j^2 \det(M_A) = (jA)^2 + (jA) + j^2 \in \mathbb{F}_{q,1}$. The fact that M_A has no fixed points on $\mathbb{P}^1(\mathbb{F}_q)$ when $A \in \mathbb{F}_q$ is shown as follows. If $M_A(w) = w$ with $w \in \mathbb{F}_q$ then $(Aw + 1/C)/(Cw + A + 1/j) = w$, which is equivalent to $(Cjw)^2 + (Cjw) + j^2 = 0$. But this would imply $\text{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(j) = 0$, a contradiction. Also $M_A(\infty) = A/C \neq \infty$ and this shows M_A has no fixed points in $\mathbb{P}^1(\mathbb{F}_q)$. Next, we show that $M_A M_B = M_K$, where $K = (1+AB)/(1/j + A + B)$. If $A = \infty$ then $K = B$ and $M_A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, so the claim is true; similarly if $B = \infty$. If A and B are both finite, then

$$M_A M_B = \begin{pmatrix} 1+AB & (A+B+1/j)/C \\ (A+B+1/j)C & 1+AB + \frac{A+B+1/j}{j} \end{pmatrix}.$$

If $A+B+1/j = 0$ then this is the identity, and also $K = \infty$ so the claim is true. If $A+B+1/j \neq 0$, then on dividing through by that constant we find

$$M_A M_B = \begin{pmatrix} \frac{1+AB}{A+B+1/j} & 1/C \\ C & \frac{1+AB}{A+B+1/j} + 1/j \end{pmatrix} = M_K.$$

To see that $\mathcal{C}_{j,C}$ is cyclic of order $q+1$, we present an isomorphism with μ_{q+1} . By Lemma 4.2, we can select $\zeta \in \mu_{q+1}$ such that $\langle \zeta \rangle = 1/j$. Let $f(M_A) = (A+1/\zeta)/(A+\zeta)$. The reader can verify that if $K = (1+AB)/(A+B+1/j)$, then

$$\frac{A+1/\zeta}{A+\zeta} \times \frac{B+1/\zeta}{B+\zeta} = \frac{K+1/\zeta}{K+\zeta},$$

and so f is a homomorphism. Also, it is one-to-one since $A \mapsto (A+1/\zeta)/(A+\zeta)$ is invertible. Finally, we note that if $\rho = (A+1/\zeta)/(A+\zeta)$, then since $\zeta^q = \zeta^{-1}$ we have $\rho^q = \rho^{-1}$. Thus, $f(M_A) \in \mu_{q+1}$. Since $|\mathcal{C}_{j,C}| = q+1 = \mu_{q+1}$ and we exhibited an injective homomorphism from $\mathcal{C}_{j,C}$ to μ_{q+1} , it must be an isomorphism and so $\mathcal{C}_{j,C}$ is cyclic. The relation (31) is straightforward to check, and this verifies the claim that $\mathcal{D}_{j,C}$ is a dihedral group of order $2(q+1)$. ■

For the remainder of this section, let $0 \neq a \in F$ where F has characteristic 2.

Proposition 7.2 *Let r, r_0, r_1 be distinct roots of $x^{q+1}+ax+a$ and $y = (r_1-r)/(r_1-r_0)$. Recall from Theorem 4.3 that each root of $C(x)+a$ can be written uniquely as $e(y, c, j)$ for some $c \in \mathbb{F}_q^\times$ and $j \in \mathbb{F}_{q,1}$, where*

$$e(y, c, j) = (cy^2 + y + j/c)^{q+1} / (y^q + y)^2.$$

For $\gamma \in \text{PGL}_2(\mathbb{F}_q)$, we have

$$e(\gamma^{-1}y, c, j) = e(y, c, j) \iff \gamma \in \mathcal{D}_{d,c/d}, \quad \text{where } d = \sqrt{j}.$$

Here, $\mathcal{D}_{j,C}$ is the dihedral group of order $2(q+1)$ that is defined by (29).

Proof. At the beginning of Section 4, we showed that if e is any root of $C(x)+a$, then there is $u \in \overline{F}$ and $\zeta, \rho \in \mu_{q+1}$ satisfying

$$1/e = \langle u^{q+1} \rangle, \quad r^2 = eT(e)^2 \langle u \rangle^{q-1}, \quad r_0^2 = eT(e)^2 \langle \zeta u \rangle^{q-1}, \quad r_1^2 = eT(e)^2 \langle \rho u \rangle^{q-1}.$$

(Note that in these formulas, we may replace (u, ζ, ρ) by $(1/u, 1/\zeta, 1/\rho)$ without affecting e, r, r_0 , and r_1 .) Further, we proved that

$$e = e(y, c, d^2), \quad \text{where } c = \frac{\langle \zeta/\rho \rangle}{\langle \zeta \rangle \langle \rho \rangle} \text{ and } d = \frac{1}{\langle \zeta \rangle}.$$

By (15) of Lemma 4.1,

$$u = T_{\zeta, \rho} y, \quad \text{where } T_{\zeta, \rho} = \begin{pmatrix} \langle \zeta/\rho \rangle & \langle \rho \rangle/\zeta \\ \langle \zeta/\rho \rangle & \langle \rho \rangle \zeta \end{pmatrix}. \quad (32)$$

Let $\gamma \in \text{PGL}_2(\mathbb{F}_q)$. Recall from Theorem 3.2 that $\gamma^{-1}(y) = (r_{\gamma(1)} - r_{\gamma(\infty)})/(r_{\gamma(1)} - r_{\gamma(0)})$. By applying the above reasoning to $\gamma^{-1}y$, we see that there are $\tilde{u}, \tilde{\zeta}$ and $\tilde{\rho}$ such that $1/e = \langle \tilde{u}^{q+1} \rangle$ and

$$e = e(\gamma^{-1}y, \tilde{c}, \tilde{d}^2), \quad \tilde{u} = T_{\tilde{\zeta}, \tilde{\rho}} \gamma^{-1}y, \quad (33)$$

where \tilde{c} and \tilde{d} have the same formula as c and d , but with ζ and ρ replaced by $\tilde{\zeta}$ and $\tilde{\rho}$. Recall also that we are free to replace $(\tilde{u}, \tilde{\zeta}, \tilde{\rho})$ by $(1/\tilde{u}, 1/\tilde{\zeta}, 1/\tilde{\rho})$. We are trying to find the condition on γ such that $(c, d) = (\tilde{c}, \tilde{d})$. So, assume $c = \tilde{c}$ and $d = \tilde{d}$. It is easy to see that $d = \tilde{d}$ if and only if $\tilde{\zeta} \in \{\zeta, \zeta^{-1}\}$. By possibly replacing \tilde{u} with its reciprocal, we may arrange that $\tilde{\zeta} = \zeta$. Then $\tilde{c} = c$ implies $\tilde{\rho} = \rho$.

Because $\langle u^{q+1} \rangle = \langle \tilde{u}^{q+1} \rangle = 1/e$, there is $\nu \in \mu_{q+1}$ such that

$$\tilde{u} = \nu^2 u \text{ or } \tilde{u} = \nu^2 / u.$$

We write this as $\tilde{u} = \nu^2 u^\varepsilon$, where $\varepsilon \in \{1, -1\}$. Then

$$\tilde{u} = Nu, \quad \text{where } N = \begin{pmatrix} \nu & 0 \\ 0 & \nu^{-1} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^\varepsilon.$$

By (32) and (33),

$$\gamma^{-1}y = T_{\zeta, \rho}^{-1}Nu = T_{\zeta, \rho}^{-1}NT_{\zeta, \rho}y. \quad (34)$$

Let $\delta^{-1} = T_{\zeta, \rho}^{-1}NT_{\zeta, \rho}$. Since $y \notin \mathbb{F}_{q^2}$ (by Theorem 3.1), an equality $\gamma^{-1}y = \delta^{-1}y$ with $\gamma, \delta \in \text{PGL}_2(\mathbb{F}_q)$ implies $\gamma = \delta$. We claim that $\delta^{-1} \in \text{PGL}_2(\mathbb{F}_q)$. Indeed, a direct computation shows that

$$\begin{aligned} T_{\zeta, \rho}^{-1} \begin{pmatrix} \nu & 0 \\ 0 & \nu^{-1} \end{pmatrix} T_{\zeta, \rho} &= \begin{pmatrix} \langle \rho \rangle \zeta & \langle \rho \rangle / \zeta \\ \langle \zeta / \rho \rangle & \langle \zeta / \rho \rangle \end{pmatrix} \begin{pmatrix} \nu \langle \zeta / \rho \rangle & \nu \langle \rho \rangle / \zeta \\ \nu^{-1} \langle \zeta / \rho \rangle & \nu^{-1} \langle \rho \rangle \zeta \end{pmatrix} \\ &= \begin{pmatrix} \langle \rho \rangle \langle \zeta / \rho \rangle \langle \zeta \nu \rangle & \langle \rho \rangle^2 \langle \nu \rangle \\ \langle \zeta / \rho \rangle^2 \langle \nu \rangle & \langle \zeta / \rho \rangle \langle \rho \rangle \langle \zeta / \nu \rangle \end{pmatrix}, \\ T_{\zeta, \rho}^{-1} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} T_{\zeta, \rho} &= \begin{pmatrix} \langle \rho \rangle \zeta & \langle \rho \rangle / \zeta \\ \langle \zeta / \rho \rangle & \langle \zeta / \rho \rangle \end{pmatrix} \begin{pmatrix} \langle \zeta / \rho \rangle & \langle \rho \rangle \zeta \\ \langle \zeta / \rho \rangle & \langle \rho \rangle / \zeta \end{pmatrix} \\ &= \begin{pmatrix} \langle \rho \rangle \langle \zeta / \rho \rangle \langle \zeta \rangle & \langle \rho \rangle^2 \langle \zeta \rangle^2 \\ 0 & \langle \rho \rangle \langle \zeta / \rho \rangle \langle \zeta \rangle \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1/c \\ 0 & 1 \end{pmatrix}, \quad \text{where } c = \frac{\langle \zeta / \rho \rangle}{\langle \zeta \rangle \langle \rho \rangle}. \end{aligned}$$

As can be seen, all entries of the above two matrices are rational and so we do indeed have $\delta^{-1} \in \text{PGL}_2(\mathbb{F}_q)$. Consequently, (34) implies that

$$\gamma^{-1} = T_{\zeta, \rho}^{-1}NT_{\zeta, \rho}.$$

Our next goal is to show that γ^{-1} belongs to $\mathcal{D}_{c/d, d}$. We do this separately for the two matrices that comprise γ^{-1} : $M_1 = T_{\zeta, \rho}^{-1} \text{diag}\{\nu, \nu^{-1}\} T_{\zeta, \rho}$ and $M_2 = T_{\zeta, \rho}^{-1} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} T_{\zeta, \rho}$. As in the discussion at the beginning of Section 7, we normalize M_1 to make $BC = 1$ and find:

$$T_{\zeta, \rho}^{-1} \begin{pmatrix} \nu & 0 \\ 0 & \nu^{-1} \end{pmatrix} T_{\zeta, \rho} = \begin{pmatrix} A & 1/C \\ C & D \end{pmatrix}, \quad \text{where } A = \frac{\langle \zeta \nu \rangle}{\langle \nu \rangle}, C = \frac{\langle \zeta / \rho \rangle}{\langle \rho \rangle}, D = \frac{\langle \zeta / \nu \rangle}{\langle \nu \rangle}.$$

Using the formula $\langle x \rangle \langle y \rangle = \langle xy \rangle + \langle x/y \rangle$, we have

$$A + D = \frac{\langle \zeta \nu \rangle + \langle \zeta / \nu \rangle}{\langle \nu \rangle} = \frac{\langle \zeta \rangle \langle \nu \rangle}{\langle \nu \rangle} = \langle \zeta \rangle = 1/d.$$

Also notice that $C = c\langle \zeta \rangle = c/d$. Thus, $M_1 \in \mathcal{D}_{d,c/d}$ as required. Since $M_2 = \begin{pmatrix} 1 & 1/c \\ 0 & 1 \end{pmatrix}$, it is immediate from (29) that $M_2 \in \mathcal{D}_{d,c/d}$ as well.

We have shown that

$$e(\gamma^{-1}y, c, d^2) = e(y, c, d^2) \text{ implies } \gamma \in \mathcal{D}_{d,c/d}. \quad (35)$$

To prove the converse, we use a counting argument. Let \mathcal{E} denote the roots of $C(x) + a$. For $e' \in \mathcal{E}$, let $H_{e'} = \{\gamma \in \text{PGL}_2(\mathbb{F}_q) : e(\gamma^{-1}y, c, d) = e'\}$. Then $\text{PGL}_2(\mathbb{F}_q)$ is the disjoint union of $H_{e'}$, for $e' \in \mathcal{E}$, and so the average size of $H_{e'}$ is $|\text{PGL}_2(\mathbb{F}_q)|/|\mathcal{E}| = q(q+1)(q-1)/\deg(C) = 2(q+1)$. On the other hand, if $\gamma_1, \gamma_2 \in H_{e'}$ then setting $y' = \gamma_2^{-1}\gamma_1 y$ we see that

$$e' = e(\gamma_1^{-1}\gamma_2 y', c, d^2) = e(y', c, d^2),$$

and so $\gamma_1^{-1}\gamma_2 \in \mathcal{D}_{d,c/d}$ by (35). Thus, $|H_{e'}| \leq |\mathcal{D}_{d,c/d}| = 2(q+1)$. Since the average size of $H_{e'}$ is $2(q+1)$, it must be that $|H_{e'}| = 2(q+1)$. In particular, $|H_e| = 2(q+1)$. By (35), we know $H_e \subset \mathcal{D}_{d,c/d}$, and by comparing cardinalities, equality must hold. ■

8. Exceptionality of $C(x)$

A polynomial $P(x) \in \mathbb{F}_r[x]$ is said to be *exceptional* over a finite field \mathbb{F}_r if it induces a permutation on K for infinitely many extension fields $K = \mathbb{F}_{r^m}$. It was proved in [2] that $C(x)$ and some related polynomials are exceptional over \mathbb{F}_2 when n is odd. Specifically, $C(x)$ induces a permutation on \mathbb{F}_{2^m} if and only if m and n are relatively prime. The first polynomials in this family were found by P. Müller with $q = 8$, degree 28. Müller's search was motivated by some deep work by Fried, Guralnick and Saxl suggesting that new examples of permutation polynomials might be found in characteristic $p = 2$ or $p = 3$ having degree $(q/2)(q-1)$, where $q = p^n$ and n is odd.

In this section we give a new proof that $C(x)$ is exceptional. We emphasize that the next proposition is known, and only the proof is new.

Proposition 8.1 *If $q = 2^n$, then $C(x) = xT(x)^{q+1}$ induces a permutation on \mathbb{F}_{2^m} if and only if $(n, 2m) = 1$.*

Proof. Note that $xT(x) = x + x^2 + \dots + x^{2^{n-1}}$, and its roots are precisely $\mathbb{F}_{2^n,0}$. Since $C(x) = xT(x)^{q+1}$, the set of roots of $C(x)$ is also $\mathbb{F}_{2^n,0}$. In particular, if $\mathbb{F}_{2^m} \cap \mathbb{F}_{2^n,0} \neq \{0\}$, then $C(x)$ is not a permutation polynomial on \mathbb{F}_{2^m} . Now $\mathbb{F}_{2^m} \cap \mathbb{F}_{2^n} = \mathbb{F}_{2^k}$ where $k = (m, n)$. Since $\mathbb{F}_{2^k,0} \subset \mathbb{F}_{2^n,0}$, we see that for $C(x)$ to be a permutation polynomial on \mathbb{F}_{2^m} , we must have $\mathbb{F}_{2^k,0} = \{0\}$, which forces $k = 1$, i.e., $(m, n) = 1$. If n is even then $1 \in \mathbb{F}_{2^m} \cap \mathbb{F}_{2^n,0}$, so another necessary condition for $C(x)$ to be a permutation polynomial on \mathbb{F}_{2^m} is that n is odd. Together, these necessary conditions may be written as $(2m, n) = 1$. Assuming this condition, then $\mathbb{F}_{2^m} \cap \mathbb{F}_q = \mathbb{F}_2$ and $\mathbb{F}_{2^m} \cap \mathbb{F}_{q,0} = \mathbb{F}_2 \cap \mathbb{F}_{q,0} = \{0\}$, so $C(x)$ has no roots in $\mathbb{F}_{2^m}^\times$. Thus, $C(x)$ sends $\mathbb{F}_{2^m}^\times$ to $\mathbb{F}_{2^m}^\times$.

From here on, let $F = \mathbb{F}_{2^m}$, where $(2m, n) = 1$. To prove that $C(x)$ is a permutation polynomial, it suffices to show that if $e \in F^\times$ and $a = C(e)$, then e is the unique root of $C(x) + a$. Suppose that e' also satisfies $a = C(e')$, and we will show that $e = e'$.

By Theorem 4.3, we have $e = e(y_0, c_0, j_0)$ for some $c_0 \in \mathbb{F}_q^\times$ and $j_0 \in \mathbb{F}_{q,1}$, where $y_0 \in \mathcal{Y}$ is the cross-ratio of any three distinct roots of $x^{q+1} + ax + a$. Since n is odd, we know $\text{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(1) = 1$, and so we may write $j_0 = 1 + b_0^2 + b_0$ for some $b_0 \in \mathbb{F}_q$. By Lemma 6.1, we have $e(y_0, c_0, j_0) = e(c_0 y_0, 1, j_0) = e(c_0 y_0 + b_0, 1, 1) = e(y, 1, 1)$, where $y = c_0 y_0 + b_0 \in \mathcal{Y}$. Then, as noted at the beginning of Section 5, e' may be written as $e(y, c, j)$ where $c \in \mathbb{F}_q^\times$ and $j \in \mathbb{F}_{q,1}$. Writing $j = 1 + b + b^2$, we see that $e' = e(cy + b, 1, 1)$. Thus,

$$e = e(y, 1, 1), \quad e' = e(cy + b, 1, 1).$$

Since e and e' are rational, they are fixed by every element of $\text{Gal}(L/F)$, where $L = F \circ \mathbb{F}_q(y)$ is the splitting field of $C(x) + a$. Since L is finite, $\text{Gal}(L/F)$ is generated by the Frobenius element:

$$\sigma(u) = u^{|F|}.$$

Since $\mathbb{F}_q \cap F = \mathbb{F}_2$, we know that if $w \in \mathbb{F}_q$, then $\sigma(w) = w$ if and only if $w \in \mathbb{F}_2$. Let γ be the element of $\text{PGL}_2(\mathbb{F}_q)$ such that $\sigma(y) = \gamma^{-1}(y)$. (Such γ exists and is unique by Theorem 3.2.) We have

$$\sigma(e) = e(\gamma^{-1}y, 1, 1), \quad \sigma(e') = e(\sigma(c)\gamma^{-1}y + \sigma(b), 1, 1).$$

Since σ fixes e and e' , we have

$$e = e(y, 1, 1) = e(\gamma^{-1}y, 1, 1), \quad e' = e(cy + b, 1, 1) = e(\sigma(c)\gamma^{-1}y + \sigma(b), 1, 1).$$

By Proposition 7.2, the first equality implies that $\gamma \in \mathcal{D}_{1,1}$; that is, $\gamma = 1$, $\gamma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, or

$$\gamma = \begin{pmatrix} A & 1 \\ 1 & A+1 \end{pmatrix} \begin{pmatrix} 1 & \varepsilon \\ 0 & 1 \end{pmatrix},$$

where $A \in \mathbb{F}_q$ and $\varepsilon \in \mathbb{F}_2$. Let $y' = cy + b$, so that $e' = e(y', 1, 1)$. Then

$$\sigma(c)\gamma^{-1}y + \sigma(b) = \delta^{-1}y', \quad \text{where} \quad \delta^{-1} = \begin{pmatrix} \sigma(c) & \sigma(b) \\ 0 & 1 \end{pmatrix} \gamma^{-1} \begin{pmatrix} c & b \\ 0 & 1 \end{pmatrix}^{-1}.$$

The fact that $e' = e(y', 1, 1) = e(\delta^{-1}y', 1, 1)$ implies that $\delta \in \mathcal{D}_{1,1}$ as well.

We may write

$$\gamma^{-1} = M_A \begin{pmatrix} 1 & \varepsilon_1 \\ 0 & 1 \end{pmatrix}, \quad \delta^{-1} = M_B \begin{pmatrix} 1 & \varepsilon_2 \\ 0 & 1 \end{pmatrix}$$

where

$$M_A = \begin{pmatrix} A & 1 \\ 1 & A+1 \end{pmatrix} \quad \text{if } A \in \mathbb{F}_q, \quad M_\infty = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

First, if $A = \infty$ (so M_A is the identity), then our relation is

$$M_B = \begin{pmatrix} \sigma(c) & \sigma(b) \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \varepsilon_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} c & b \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & \varepsilon_2 \\ 0 & 1 \end{pmatrix}.$$

Since the bottom left entry is 0, we have $M_B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. The right side is

$$\begin{pmatrix} \sigma(c) & \sigma(c)(\varepsilon_2 + b) + c(\varepsilon_1\sigma(c) + \sigma(b)) \\ 0 & c \end{pmatrix}.$$

For this to be the identity, we need $c = \sigma(c)$. Since the fixed field of σ is F , we obtain $c \in F^\times \cap \mathbb{F}_q = \mathbb{F}_2^\times = \{1\}$. Setting $c = 1$, we find the top-right entry is $\varepsilon_1 + \varepsilon_2 + b + \sigma(b)$, and so $b + \sigma(b) \in \mathbb{F}_2$. If $b + \sigma(b) = 1$, then we'd have $\text{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(b + \sigma(b)) = \text{Tr}(1)$, or $0 = 1$, a contradiction. So $b = \sigma(b)$, and $b \in \mathbb{F}_2$. Then $j = 1 + b + b^2 = 1$, and so $e' = e(y, c, j) = e(y, 1, 1) = e$, as we wanted to show.

Now suppose $A \in \mathbb{F}_q$. Then we obtain an equation

$$M_B = \begin{pmatrix} \sigma(c) & \sigma(b) \\ 0 & 1 \end{pmatrix} M_A \begin{pmatrix} 1 & \varepsilon_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} c & b \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & \varepsilon_2 \\ 0 & 1 \end{pmatrix}.$$

The right side is

$$\begin{pmatrix} \sigma(c)A + \sigma(b) & (\sigma(c)A + \sigma(b))(\varepsilon_1c + b + \varepsilon_2) + (\sigma(c) + \sigma(b)A + \sigma(b))c \\ 1 & \varepsilon_1c + b + \varepsilon_2 + Ac + c \end{pmatrix}.$$

To be of the form M_B , we require that the top-right entry is 1 and the trace is 1. This gives the two equalities:

$$(\sigma(c)A + \sigma(b))(\varepsilon_1c + b + \varepsilon_2) + (\sigma(c) + \sigma(b)A + \sigma(b))c = 1 \quad (36)$$

$$(c + \sigma(c))A + (\varepsilon_1 + 1)c + \sigma(b) + b + \varepsilon_2 = 1. \quad (37)$$

First, if $c + \sigma(c) = 0$, then we will have $c \in F^\times \cap \mathbb{F}_q = \mathbb{F}_2^\times$. Substituting $c = 1$, we find as before that $b \in \mathbb{F}_2$ and obtain $e = e'$ in the same way as before.

Next assume $c + \sigma(c) \neq 0$, and we will obtain a contradiction. Multiply through (36) by $c + \sigma(c)$, and then use $(c + \sigma(c))A = (\varepsilon_1 + 1)c + \sigma(b) + b + \varepsilon_2 + 1$ in order to eliminate A from (36). After simplifying, we obtain:

$$\sigma(b)^2c + b^2\sigma(c) + \sigma(b)c + b\sigma(c) + (b + \varepsilon_1 + \sigma(b) + \varepsilon_2)c\sigma(c) + (c + \sigma(c))(c\sigma(c) + 1) = 0.$$

On dividing by $c\sigma(c)$, we find that $x + \sigma(x) = \varepsilon_1 + \varepsilon_2 \in \mathbb{F}_2$, where

$$x = b^2/c + b/c + b + c + 1/c.$$

Since $\text{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(x + \sigma(x) + \varepsilon_1 + \varepsilon_2) = \varepsilon_1 + \varepsilon_2$, we must have $\varepsilon_1 = \varepsilon_2$. Thus, $\sigma(x) = x$ and consequently $x \in \mathbb{F}_2$.

If $x = 0$, we find that $b^2 + b(c + 1) + c^2 + 1 = 0$. Since we are assuming $c \neq \sigma(c)$, we may divide through by $(c + 1)^2$ and this gives

$$\left(\frac{b}{c+1}\right)^2 + \frac{b}{c+1} + 1 = 0.$$

Then $\text{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(1) = 0$, a contradiction since n is odd.

If $x = 1$, we find that $b^2 + bc + b + c^2 + 1 = c$. If $b = c$ then $c^2 + c^2 + c + c^2 + 1 = c$, so $c = 1$, a contradiction since we are in the case $c \neq \sigma(c)$. So we may divide through by $(b + c)^2$, and we find

$$0 = \frac{b^2 + c^2 + b + c + 1 + bc}{(b + c)^2} = 1 + \frac{c + 1}{b + c} + \left(\frac{c + 1}{b + c}\right)^2.$$

On taking the trace, we obtain $0 = \text{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(1)$, a contradiction since n is odd. The contradiction shows that $c + \sigma(c)$ must be 0, and we already showed that implies $e = e'$. We conclude that $C(e) + a = C(e') + a$ implies $e = e'$, so $C(x)$ is indeed a permutation polynomial when $(2n, m) = 1$. ■

References

- [1] Shereem S. Abhyankar, Stephen D. Cohen, and Michael E. Zieve, *Bivariate factorizations connecting Dickson polynomials and Galois theory*, Transactions of the American Mathematical Society, Vol. 352, No. 6, 2871–2887, February 2000.
- [2] Stephen D. Cohen and Rex W. Matthews, *A class of exceptional polynomials*, Transactions of the American Mathematical Society, Vol. 345, No. 2, 897–909, October 1994.
- [3] Leonard Eugene Dickson, *Linear Groups with an Exposition of the Galois Theory*, Dover Publications, 1958.
- [4] D. S. Dummit, *Solving solvable quintics*, Mathematics of Computation **57**, No. 195, 387–401, July 1991.
- [5] Antonia W. Bluher, *On $x^{q+1} + ax + b$* , Finite Fields and Their Applications **10**, 285–305, 2004.
- [6] Robert M. Guralnick, Joel E. Rosenberg, and Michael E. Zieve, *A new family of exceptional polynomials in characteristic two*, Annals of Mathematics, 2010.
- [7] Robert M. Guralnick and Michael E. Zieve, *Polynomials with $PSL(2)$ monodromy*, Ann. Math **172**, 1321–1365, 2010.
- [8] H. W. Lenstra, Jr. and M. Zieve, *A family of exceptional polynomials in characteristic three*, in: Finite Fields and Applications (ed. S. Cohen and H. Niederreiter), Cambridge Univ. Press, Lecture Note Series of the London Mathematical Society **233**, 209–218, 1996.
- [9] M. Zieve, *Bivariate factorizations via Galois theory, with application to exceptional polynomials*, J. Algebra **210**, 670–689, 1998.
- [10] P. Müller, *New examples of exceptional polynomials*, in *Finite Fields: Theory, Applications and Algorithms*, Amer. Math. Soc., Providence, 245–249, 1994.